

Blockchain & Cryptocurrency Regulation

2021

Third Edition

Contributing Editor: **Josias N. Dewey**

glg global legal group



Global Legal Insights Blockchain & Cryptocurrency Regulation

2021, Third Edition

Contributing Editor: Josias N. Dewey

Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – BLOCKCHAIN & CRYPTOCURRENCY REGULATION

2021, THIRD EDITION

Contributing Editor
Josias N. Dewey, Holland & Knight LLP

Head of Production
Suzie Levy

Senior Editor
Sam Friend

Sub Editor
Megan Hylton

Consulting Group Publisher
Rory Smith

Chief Media Officer
Fraser Allan

*We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Josias N. Dewey of Holland & Knight LLP for all of his assistance.*

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

Copyright © 2020
Global Legal Group Ltd. All rights reserved
No photocopying

ISBN 978-1-83918-077-4
ISSN 2631-2999

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication. This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations. The information contained herein is accurate as of the date of publication.

Printed and bound by TJ International, Treceus Industrial Estate, Padstow, Cornwall, PL28 8RW
October 2020

CONTENTS

Preface	Josias N. Dewey, <i>Holland & Knight LLP</i>	
Foreword	Aaron Wright, <i>Enterprise Ethereum Alliance</i>	
Glossary	The Editor shares key concepts and definitions of blockchain	
Industry	<i>Five years of promoting innovation through education: The blockchain industry, law enforcement and regulators work towards a common goal</i> Jason Weinstein & Alan Cohn, <i>The Blockchain Alliance</i>	1
	<i>The loan market, blockchain, and smart contracts: The potential for transformative change</i> Bridget Marsh, <i>LSTA & Josias N. Dewey, Holland & Knight LLP</i>	5
	<i>Progress in a year of mayhem – Blockchain, cryptoassets and the evolution of global markets</i> Ron Quaranta, <i>Wall Street Blockchain Alliance</i>	14
	<i>Cryptocurrency and blockchain in the 116th Congress</i> Jason Brett & Whitney Kalmbach, <i>Value Technology Foundation</i>	20
General chapters	<i>Blockchain and intellectual property: A case study</i> Joshua Krumholz, Ieuan G. Mahony & Brian J. Colandreo, <i>Holland & Knight LLP</i>	38
	<i>Cryptocurrency and other digital asset funds for U.S. investors</i> Gregory S. Rowland & Trevor I. Kiviat, <i>Davis Polk & Wardwell LLP</i>	54
	<i>Not in Kansas anymore: The current state of consumer token regulation in the United States</i> David L. Concannon, Yvette D. Valdez & Stephen P. Wink, <i>Latham & Watkins LLP</i>	68
	<i>An introduction to virtual currency money transmission regulation</i> Michelle Ann Gitlitz, Carlton Greene & Caroline Brown, <i>Crowell & Moring LLP</i>	93
	<i>Cryptocurrency compliance and risks: A European KYC/AML perspective</i> Fedor Poskriakov, Maria Chiriaeva & Christophe Cavin, <i>Lenz & Staehelin</i>	111
	<i>Decentralized Finance: Have digital assets and open blockchain networks found their “killer app”?</i> Lewis Cohen, Angela Angelovska-Wilson & Greg Strong, <i>DLx Law</i>	126
	<i>Legal issues surrounding the use of smart contracts</i> Stuart Levi, Cristina Vasile & MacKinzie Neal, <i>Skadden, Arps, Slate, Meagher & Flom LLP</i>	148
	<i>Distributed ledger technology as a tool for streamlining transactions</i> Douglas Landy, James Kong & Jonathan Edwards, <i>Milbank LLP</i>	165
	<i>Blockchain M&A: The next link in the chain</i> F. Dario de Martino, <i>Morrison & Foerster LLP</i>	178
	<i>Untying the Gordian Knot – Custody of digital assets</i> Richard B. Levin, David M. Allred & Peter F. Waltz, <i>Polsinelli PC</i>	197

Country chapters

Australia	Peter Reeves & Emily Shen, <i>Gilbert + Tobin</i>	210
Austria	Ursula Rath & Thomas Kulnigg, <i>Schönherr Rechtsanwälte GmbH</i>	222
Canada	Simon Grant, Kwang Lim & Matthew Peters, <i>Bennett Jones LLP</i>	229
Cayman Islands	Alistair Russell & Jenna Willis, <i>Carey Olsen</i>	242
Cyprus	Akis Papakyriacou, <i>Akis Papakyriacou LLC</i>	250
Gibraltar	Joey Garcia & Jonathan Garcia, <i>ISOLAS LLP</i>	257
Hong Kong	Yu Pui Hang (Henry Yu), <i>L&Y Law Office / Henry Yu & Associates</i>	266
Ireland	Keith Waine, Karen Jennings & David Lawless, <i>Dillon Eustace</i>	280
Italy	Massimo Donna & Lavinia Carmen Di Maria, <i>Paradigma – Law & Strategy</i>	289
Japan	Taro Awataguchi & Takeshi Nagase, <i>Anderson Mōri & Tomotsune</i>	295
Jersey	Christopher Griffin, Emma German & Holly Brown, <i>Carey Olsen Jersey LLP</i>	306
Luxembourg	José Pascual, Holger Holle & Clément Petit, <i>Eversheds Sutherland LLP</i>	312
Mexico	Carlos David Valderrama Narváez, Alejandro Osornio Sánchez & Diego Montes Serralde, <i>Legal Paradox®</i>	320
Montenegro	Jovan Barović, Luka Veljović & Petar Vučinić, <i>Moravčević Vojnović i Partneri AOD in cooperation with Schoenherr</i>	327
Portugal	Filipe Lowndes Marques & Mariana Albuquerque, <i>Morais Leitão, Galvão Teles, Soares da Silva & Associados</i>	332
Serbia	Bojan Rajić & Mina Mihaljčić, <i>Moravčević Vojnović i Partneri AOD Beograd in cooperation with Schoenherr</i>	342
Switzerland	Daniel Haerberli, Stefan Oesterhelt & Alexander Wherlock, <i>Homburger AG</i>	348
Taiwan	Robin Chang & Eddie Hsiung, <i>Lee and Li, Attorneys-at-Law</i>	363
United Kingdom	Stuart Davis, Sam Maxson & Andrew Moyle, <i>Latham & Watkins LLP</i>	369
USA	Josias N. Dewey, <i>Holland & Knight LLP</i>	384

PREFACE

Another year has passed and virtual currency and other blockchain-based digital assets continue to attract the attention of policymakers across the globe. A lack of consistency in how policymakers are addressing concerns raised by the technology is a major challenge for legal professionals who practice in this area. Perhaps equally challenging is keeping up with the nearly infinite number of blockchain use cases. In 2017 and 2018, it was the ICO craze. In 2019, the focus shifted to security tokens. In 2020, decentralized finance (or DeFi) attracted over several billion dollars' worth of investment. So, while ICOs are still being offered and several groups continue to pursue serious security token projects, we should expect DeFi to draw scrutiny from regulators, such as the U.S. Securities and Exchange Commission (SEC). Once again, legal practitioners will be left to counsel clients on novel issues of law raised by the application of laws and regulations enacted long before blockchain technology existed.

Of course, capital raising is only one application of the technology. Bitcoin, which remains the king of all cryptocurrencies, was intended to serve as a form of digital money. Arguably, it is this use case that has seen the most attention from governments around the world. The European Union enacted more stringent anti-money laundering (AML) regulations impacting virtual currency exchanges operating in the EU. U.S. regulators and state government officials continue to enforce money transmitter statutes and BSA regulations applicable to money services businesses. In the U.S., the state of New York, which was once thought to have over-regulated the industry out of doing business in the state, is now attracting applications from blockchain companies to become state-chartered trust companies. The charter may provide relief to virtual currency exchanges and similar businesses seeking to avoid the nearly 50-state patchwork of licensing statutes.

Institutional and large enterprise companies continue to expand into the space. It is no longer just FinTechs and entrepreneurial clients who need counsel on blockchain-related matters. Whether a small start-up or Fortune 100 company, clients need counsel in areas beyond compliance with government regulation. In some cases, intellectual property rights must be secured, or open source licenses considered to the extent a client's product incorporates open source code. Blockchain technology adopted by enterprise clients may involve a consortium of prospective network users, which raises joint development issues and governance questions.

As with the first two editions, our hope is that this publication will provide the reader with an overview of the most important issues across many different use cases and how those issues are impacted by laws and regulations in several dozen jurisdictions around the globe. And while policymakers continue to balance their desire to foster innovation, while protecting the public interest, readers of this publication will understand the current state of affairs, whether in the U.S., the EU, or elsewhere in the world. Readers may even discover themes across this book's chapters that provide clues about what we can expect to be the hot topics of tomorrow and beyond.

Josias N. Dewey
Holland & Knight LLP

FOREWORD

Dear Industry Colleagues,

On behalf of the Enterprise Ethereum Alliance (“EEA”), I would like to thank Global Legal Group (“GLG”) for bringing to life an explication of the state of regulation in the blockchain and cryptocurrency sector, with its third edition publication of *Blockchain & Cryptocurrency Regulation*. GLG has assembled a remarkable group of leaders in the legal industry to analyse and explain the environment in front of us, and the EEA members and participants were pleased to contribute to the publication.

We stand at the beginning of an industry, and the depth and breadth of the contributors from leading law firms across the world only serve to highlight the growing interest and fascination with accelerating the adoption of blockchain technology. We thank each of the authors for taking the time to compose their chapters and for the expertise they demonstrate. We hope readers will find this publication useful.

The EEA is the industry’s first member-driven global standards organisation whose mission is to develop open, blockchain specifications that drive harmonisation and interoperability for businesses and consumers worldwide. The EEA’s world-class Enterprise Ethereum Client Specification, Off-Chain Trusted Compute Specification, and forthcoming testing and certification programs, along with its work with the Token Taxonomy Initiative, will ensure interoperability, multiple vendors of choice, and lower costs for its members – hundreds of the world’s largest enterprises and most innovative startups. For additional information about joining the EEA or the Token Taxonomy Initiative, please reach out to membership@entethalliance.org and info@tokentaxonomy.org.

Sincerely,

Aaron Wright

Chairman, EEA Legal Advisory Working Group

GLOSSARY

Alice decision: a 2014 United States Supreme Court decision about patentable subject matter.

Cold storage: refers to the storage of private keys on an un-networked device or on paper in a secure location.

Copyright licence: the practice of offering people the right to freely distribute copies and modified versions of a work with the stipulation that the same rights be preserved in derivative works down the line.

Cryptocurrencies: a term used interchangeably with virtual currency, and generally intended to include the following virtual currencies (and others similar to these):

- Bitcoin.
- Bitcoin Cash.
- DASH.
- Dogecoin.
- Ether.
- Ethereum Classic.
- Litecoin.
- Monero.
- NEO.
- Ripple's XRP.
- Zcash.

Cryptography: the practice and study of techniques for secure communication in the presence of third parties, generally involving encryption and cyphers.

DAO Report: report issued in July, 2017 by the U.S. Securities and Exchange Commission, considering and ultimately concluding that The DAO (*see below*) was a security.

Decentralised autonomous organisation (“The DAO”): a failed investor-directed venture capital fund with no conventional management structure or board of directors that was launched with a defect in its code that permitted someone to withdraw a substantial amount of the \$130,000,000 in Ether it raised.

Decentralised autonomous organisation (“a DAO”): a form of business organisation relying on a smart contract (*see below*) *in lieu* of a conventional management structure or board of directors.

Digital assets: anything that exists in a binary format and comes with the right to use, and more typically consisting of a data structure intended to describe attributes and rights associated with some entitlement.

Digital collectibles: digital assets that are collected by hobbyists and others for entertainment, and which are often not fungible (e.g., CryptoKitties) (*see Tokens*, non-fungible).

Digital currency: a type of currency available only in digital form, which can be fiat currency or virtual currency that acts as a substitute for fiat currency.

Digital currency exchange: a business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money, or one type of cryptocurrency for another type of cryptocurrency.

Digital/electronic wallet: an electronic device or software that allows an individual to securely store private keys and broadcast transactions across a peer-to-peer network, which can be hosted (e.g., Coinbase) or user managed (e.g., MyEtherWallet).

Distributed ledger technology (“DLT”): often used interchangeably with the term *blockchain*, but while all blockchains are a type of DLT, not all DLTs implement a blockchain style of achieving consensus.

Fintech: new technology and innovation that aims to compete with traditional financial methods in the delivery of financial services.

Initial coin offering: a type of crowdfunding using cryptocurrencies in which a quantity of the crowdfunded cryptocurrency is sold to either investors or consumers, or both, in the form of “tokens”.

Initial token offering: *see Initial coin offering*.

Internet of Things: a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Licences, software: the grant of a right to use otherwise copyrighted code, including, among others:

- Apache.
- GPLv3.
- MIT.

Mining, cryptocurrency: the process by which transactions are verified and added to the public ledger known as the blockchain, which is often the means through which new units of a virtual currency are created (e.g., Bitcoin).

Money transmitter (U.S.): a business entity that provides money transfer services or payment instruments.

Permissioned network: a blockchain in which the network owner(s) decides who can join the network and issue credentials necessary to access the network.

Platform or protocol coins: the native virtual currencies transferable on a blockchain network, which exist as a function of the protocol's code base.

Private key: an alphanumeric cryptographic key that is generated in pairs with a corresponding public key. One can verify possession of a private key that corresponds to its public key counterpart without exposing it. It is not possible, however, to derive the private key from the public key.

Private key storage:

- *Deep cold storage:* a type of cold storage where not only Bitcoins are stored offline, but also the system that holds the Bitcoins is never online or connected to any kind of network.
- *Hardware wallet:* an electronic device capable of running software necessary to store private keys in a secure, encrypted state and structure transactions capable of being broadcast on one or more blockchain networks. Two popular examples are Ledger and Trezor.

Protocols: specific code bases implementing a particular blockchain network, such as:

- Bitcoin.
- R3's Corda.
- Ethereum.
- Hyperledger Fabric.
- Litecoin.

Public network: blockchain that anyone can join by installing client software on a computer with an internet connection. Best known public networks are Bitcoin and Ethereum.

Qualified custodian: a regulated custodian who provides clients with segregated accounts and often places coins or tokens in cold storage (*see above*).

Robo-advice/digital advice: a class of financial adviser that provides financial advice or investment management online, with moderate to minimal human intervention.

Sandbox (regulatory): a programme implemented by a regulatory agency that permits innovative start-ups to engage in certain activities that might otherwise require licensing with one or more governmental agencies.

Security token: a token intended to confer rights typically associated with a security (e.g., stock or bond), and hence, are generally treated as such by regulators.

Smart contract: a piece of code that is written for execution within a blockchain runtime environment. Such programmes are often written to automate certain actions on the network, such as the transfer of virtual currency if certain conditions in the code are met.

Tokens: a data structure capable of being fungible (ERC-20) or non-fungible (ERC-721) that is capable of being controlled by a person to the exclusion of others, which is typically transferable from one person to another on a blockchain network.

Utility token: a token intended to entitle the holder to consume some good or service offered through a decentralised application ("dApp").

Vending machine (Bitcoin): an internet machine that allows a person to exchange Bitcoins and cash. Some Bitcoin ATMs offer bi-directional functionality, enabling both the purchase of Bitcoin as well as the redemption of Bitcoin for cash.

Five years of promoting innovation through education:

The blockchain industry, law enforcement and regulators work towards a common goal

Jason Weinstein & Alan Cohn
The Blockchain Alliance

Criminal use of technology

When many people think of “bitcoin” or other cryptocurrencies, they often think of crime, because of “Silk Road” and other high-profile examples of people exploiting cryptocurrencies for unlawful purposes.

But for the entrepreneurs, engineers, venture capitalists and bankers who are pouring their time, energy, and money into cryptocurrency- and cryptoasset-related businesses, the technology – whether the assets themselves, the ability to build decentralised financial services applications, or the underlying blockchain technology – continues to grow and thrive, and drive innovation. And contrary to popular belief, this technology is friendlier to law-enforcers than it is to law-breakers.

Blockchain technology uses cryptography to verify and confirm all transactions and then records those transactions on a searchable public ledger. Bitcoin and other cryptocurrencies represent just the first “app” for blockchain technology. There are endless other possibilities for that technology – from securities and commodities trading, to decentralised financial applications, to supply chain management, to IP rights, to identity management and security, to real estate to government services, just to name a few – that could transform the way the world does business, much like the internet did over 20 years ago.

It is a fact of life in law enforcement that criminals are always among the first adopters of any novel technology that works. And law enforcement has a long history of adapting in order to pursue criminals who use “new school” technology to commit “old school” crimes. From beepers to email to online chat to Skype to social networking, law enforcement consistently has had to evolve as new technology designed for legitimate purposes is used to facilitate criminal activity. Bitcoin and other cryptocurrencies represent just the latest example.

While there is unquestionably criminal activity taking place via the internet, we do not think of the internet as the “computer network of criminals”. That is because the vast majority of commercial activity over the internet is legitimate, whereas illicit activity facilitated by the web represents just a small portion of what happens on the internet every day. Similarly, bitcoin and other cryptocurrencies should not be thought of as “currencies of criminals”, because illicit transactions, while they exist, account for only a minute portion of the activity involving this new technology. Moreover, this technology has more potential to help root out money laundering and terrorism financing as it does to enable these types of activities.

Proactive engagement by industry

Recognising a shared interest in helping combat criminal exploitation of this revolutionary technology, five years ago the blockchain and cryptocurrency industry proactively

approached law enforcement and regulatory agencies and offered to help educate these agencies about how cryptocurrencies work, provide technical assistance and an understanding of industry best practices, and foster an open dialogue about issues of common concern. Under the leadership of the Chamber of Digital Commerce and Coin Center, the industry established the Blockchain Alliance, a non-profit organisation administered by Steptoe & Johnson LLP that serves as a forum for engagement between the blockchain industry and law enforcement and regulatory agencies. Since its founding in 2015, the Blockchain Alliance has grown to include over 100 blockchain and cryptocurrency companies and law enforcement and regulatory agencies in the U.S. and around the world, including Europol and Interpol and authorities in Europe, Latin America, Africa, Asia, and Australia. In 2020, the Blockchain Alliance added programming specifically for compliance officials at the world's largest banks, helping to introduce those officials to the blockchain and cryptocurrency industry and to the compliance solutions that exist to help handle this new technology safely and efficiently.

Through the Blockchain Alliance, some of the brightest minds in the industry are working with law enforcement and regulatory agencies to combat criminal activity involving this new technology, in an effort to promote public safety and a pro-innovation regulatory environment. The Blockchain Alliance convenes regular calls to discuss trends in the industry and tools for combatting criminal activity. The Alliance has conducted educational programmes for nearly 700 law enforcement officers and regulators from more than 35 countries. These educational programmes cover a range of topics from the basics of the technology, to tracing tools, to privacy coins. Finally, the Alliance provides mechanisms for law enforcement and regulatory agencies to connect directly with industry on matters of common concern.

Tracing the flow of funds

One of the main misconceptions Blockchain Alliance members have worked to correct is that bitcoin transactions are anonymous. The reality is that the technology has significant benefits for investigators seeking to “follow the (digital) money”. Having a public, traceable, immutable, borderless ledger of every transaction ever conducted allows law enforcement to trace the flow of funds involving an investigative target anywhere in the world in a way that would not be possible with cash or many other types of financial instruments. And industry has developed software tools for connecting bitcoin addresses to a particular user – similar to the challenge law enforcement has faced for years trying to identify anonymous hackers and other cybercriminals – and those tools are continually improving, as well as expanding for use with respect to other cryptocurrencies. Those same types of tools allow cryptocurrency exchanges and others to better identify suspicious actors and transactions as part of their anti-money laundering (“AML”) compliance programmes. Under the circumstances, criminals should be running, not walking, away from using bitcoin and other types of cryptocurrencies.

Impact of regulation

While it is often said that cryptocurrencies and blockchain technology are unregulated, nothing could be further from the truth. Numerous federal and state agencies in the U.S., as well as agencies in other countries, regulate applications for this technology in some fashion. But the disparate approaches taken by different countries, or even by different agencies within the U.S., have led to confusion on the part of blockchain companies about the jurisdictions and regulatory regimes to which their products and services will be subject.

Many jurisdictions, even within the U.S., regulate cryptocurrency activities like the exchange of cryptocurrency to fiat, or cryptocurrency to cryptocurrency, differently. Europe has now adopted regulation to include cryptocurrency companies like exchanges within the scope of the 5th Anti-Money Laundering Directive. Some exchanges offering services that do not clearly fit in the current regulatory regime have voluntarily developed robust procedures in order to verify their customers' identity and the source of funds. These "on-ramps" and "off-ramps" to the cryptocurrency economy provide law enforcement, regulatory agencies, and traditional financial institutions with insights concerning the cryptocurrency economy as well as places to check and monitor transactions back and forth between cryptocurrency and fiat currencies. Indeed, key trendlines continue to indicate that AML measures are getting more stringent, but that criminals are continuing to look for ways to evade effective AML activities. For example, the blockchain forensics and cryptocurrency analytics provider CipherTrace, a Blockchain Alliance member, estimates that "the global average of criminal funds sent directly to exchanges dropped 47% in 2019", which "suggests that many criminals are finding it harder to offload their illicit funds directly into cryptocurrency exchanges".¹ However, clear regulations and guidelines on AML and know-your-customer policies can help further reduce the criminal activity flowing through exchanges and other cryptocurrency companies.

Moving forward through continued engagement

In order to ensure the growth of the industry while also protecting consumers and preventing money laundering, a pro-innovation approach to regulation is needed. Positive and proactive engagement by industry with law enforcement and regulators, through the Blockchain Alliance and otherwise, has been critical to the growth of this sector to date. Continued engagement of this type will be equally important going forward, as industry seeks to foster an approach to lawmaking and rulemaking that encourages, rather than stifles, innovation. Only then can the full potential of blockchain technology be realised.

* * *

Endnote

1. CipherTrace, Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report, <https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/>.

**Jason Weinstein, Director****Tel: +1 202 429 8061 / Email: jweinstein@step toe.com**

Jason Weinstein is Partner at Steptoe & Johnson LLP, co-chair of the firm's Blockchain and Cryptocurrency practice, and Director to the Blockchain Alliance. He has represented just about every type of participant in the blockchain ecosystem and is widely recognised as one of the leading defence attorneys in government enforcement matters relating to cryptocurrencies. Jason previously served as deputy assistant attorney general in the Department of Justice's Criminal Division, where he supervised the computer crime and organised crime sections, and oversaw numerous investigations involving the use of digital currencies. Jason serves on the advisory boards of Coin Center and the Chamber of Digital Commerce. He also serves as an advisor to Bitfury, the leading full-service blockchain technology company and one of the largest private infrastructure providers in the industry.

**Alan Cohn, Counsel****Tel: +1 202 429 6283 / Email: acohn@step toe.com**

Alan Cohn is Partner at Steptoe & Johnson LLP, co-chair of the firm's Blockchain and Cryptocurrency practice, and Counsel to the Blockchain Alliance. Alan counsels companies on cybersecurity, blockchain and distributed ledger technology, and national security issues. Alan is ranked among the top U.S. lawyers in Blockchain and Cryptocurrencies by *Chambers USA* (2019–2020), where he is noted for his “tremendous depth of expertise in regulatory issues facing blockchain platforms and cryptocurrencies”. He previously served in senior policy and management positions at the U.S. Department of Homeland Security for almost a decade, most recently as the Assistant Secretary for Strategy, Planning, Analysis & Risk and second-in-charge overall of the DHS Office of Policy. Alan also serves as an advisor to several technology companies.

The Blockchain Alliance

1330 Connecticut Avenue, NW, Washington, D.C. 20036, USA

URL: www.blockchainalliance.org

The loan market, blockchain, and smart contracts: The potential for transformative change

Bridget Marsh, LSTA
Josias N. Dewey, Holland & Knight LLP

Introduction

The Loan Syndications and Trading Association (“LSTA”) is the trade association in the United States for the corporate loan market. We promote a fair, orderly, and efficient loan market and actively seek ways in which we can achieve that. During the past few years, the LSTA has considered how blockchain (or distributed ledger technology (“DLT”)) and related advanced technologies will impact the industry and believes that this new technology can propel the syndicated loan market forward and help address some of its current challenges.

This chapter provides a brief description of the loan market and its participants to put our conversation in context, sets out the basics of blockchain technology, reviews the concept of “smart contracts”, and examines how the primary and secondary loan markets can benefit from these new technologies.

U.S. loan market and loan market participants

There is no single regulatory authority charged with the responsibility of regulating the syndicated loan market in the United States. Of course, most loan market participants are regulated institutions that have one or more regulators overseeing their activities, but the loan market itself is not regulated. The LSTA is, therefore, the entity to which loan market participants turn for standard forms, best practices, and general assistance with primary loan market activities and secondary market loan trades.

The LSTA maintains a suite of documents that can be used by market participants in the origination, servicing, and trading of loans. Since its formation 25 years ago, the LSTA has published standard agreements, forms, and best practices for use in the primary loan market which have been widely adopted by market participants. The LSTA’s comprehensive suite of secondary trading documents are used by all loan market participants to evidence their loan trades and then settle those transactions.

At its most basic, in the primary loan market, there are several interested parties involved in the origination of any large syndicated loan, the terms of which are documented in a credit agreement. There must be: (i) a borrower to which the loan is made and which is responsible for principal and interest payments under the terms of the credit agreement; (ii) one or more lenders in the syndicate, each of which owns a portion of the outstanding loan; and (iii) an administrative agent which is responsible for the ongoing administration of the loan until its maturity date. Although complex deal terms may vary from deal to deal, the basics of each loan will generally operate the same way. In the secondary loan market, each loan trade will, of course, include a selling lender and a legal entity buying the loan, an administrative agent who must acknowledge or consent to the loan assignment,

and a borrower whose consent to the loan trade is also typically required. The buyer and seller of the loan execute an LSTA Par/Near Par Trade Confirmation (“LSTA Confirm”) to evidence their loan trade, and the relevant form of assignment agreement pursuant to which the loan is then assigned to the buyer. Finally, the administrative agent updates the register of lenders to reflect the loan assignment.

For the trading of performing loans (“par trades”) where the borrower is making timely loan payments in accordance with the terms of the credit agreement and neither the borrower nor the applicable industry is in any type of financial distress or experiencing any type of turmoil, most of the steps outlined above have become standard practice in the U.S. loan market, and LSTA trading documentation is used uniformly by all participants. After the relevant consents are obtained, those par trades are typically settled on an electronic platform with little or no lawyer involvement and few, if any, modifications. Instead, market participants expect the LSTA to provide the market with trading documents that are periodically updated to reflect current market practices, legal developments, and the latest deal trends.

Because there is no (or very limited) tailoring of documents in the trading of par loans and with practices being quite streamlined and uniform, distinct elements of this market seem ideally suited for the implementation of blockchain technology.

Blockchain basics

The terms blockchain and DLT are often used interchangeably by those in financial services, and both terms seem to be used as acceptable nomenclature for this technology. Although there is a technical distinction between a blockchain and a DLT, for the purposes of our discussion, the terms will be used interchangeably, although it seems that the term “blockchain” is the preferred term today by those in financial services.

Perhaps surprising to some is that the technology underlying blockchain is actually a collection of technologies none of which is new. Blockchain is a decentralised, peer-to-peer network that maintains a ledger of transactions (e.g., a transfer of an asset from one party to another party) that uses cryptographic tools to maintain the integrity of transactions and the integrity of the ledger itself, and a protocol-wide consensus mechanism that verifies the data and determines if, when, and how to update the ledger. The decentralised network makes this technology distinct from a traditional centralised database that has one authoritative database maintained by a trusted third party. For example, central banks around the world serve as that trusted third party for a state’s banking system; similarly, for a syndicated loan, the administrative agent is the trusted third party that maintains the register of lenders, administers the loan, and keeps a record of all loan positions, including related interest and principal payments. Lenders in the syndicate must reconcile their own records with those of the administrative agent whose entries in the register are conclusive, absent manifest error. Without a trusted party to maintain a ledger, by contrast, in a blockchain, the cryptographic tools (e.g., a public or private encryption key) keep the information secure, for they are used to control the ownership of and/or the right to access the information on the ledger.

A blockchain is often considered to be immutable or tamper-proof because of the technology used to maintain the integrity of the ledger. Although there have been a few examples of hacking of digital currencies that rely on this technology, the unique way in which the information is stored and updated does make it incredibly secure, so it is most definitely tamper-resistant. For example, to create each “block” in a blockchain, transactions are aggregated together and, using the appropriate protocol (a protocol can be thought of as software or a set of rules for a particular system), subjected to a special mathematical

algorithm. The calculation results in an alphanumeric string that is put on the next block, and those two blocks are now inextricably chained together, or “cryptographically linked”. The process is then repeated for each bundle of transactions that are aggregated together; the number of blocks will increase, and the chain will continue to grow over time. To tamper or attempt to hack into or change some of the stored information would be nearly impossible and incredibly expensive. Because a new entry on a blockchain ledger is verified by a consensus mechanism at the time of entry and updated across all computers simultaneously, the computers rely on and trust this single source of truth. One of the enormous benefits of this technology is the potential for cost savings because separate reconciliation efforts will no longer be needed. (This alone makes it incredibly attractive technology for the loan market.)

Public or permissioned ledger

DLT can be implemented with or without access controls, depending on whether an open, public network is used or a restricted, permissioned network is chosen. The decentralised digital currency, Bitcoin, is likely the most well-known example of an open, public network where anyone can query the ledger and broadcast transactions without any authorisation (assuming, of course, the individual has the proper computer equipment and software). In a public blockchain, ledgers are replicated across many computers referred to as “nodes”, which are connected to a common network over the internet. Those operating the nodes are referred to as “miners”. In contrast, a closed, permissioned network is restricted to certain individuals who have been given permission and the necessary credentials to access the ledger by a trusted third party.

It is not surprising that the financial services industry is currently favouring the implementation of permissioned networks. Because of anti-money laundering (“AML”), know-your-customer (“KYC”), and privacy considerations (discussed more fully below), public networks are not really feasible in financial services at this time. A Bitcoin miner that is anonymous on a public network should be subject to the requirements of the Bank Secrecy Act and a financial institution’s own KYC programme as if it were to be involved in a similar function in the financial services industry for a bank. Thus, it is unlikely that financial institutions would rely entirely on public blockchain networks as the infrastructure underlying a loan origination or trading platform. As the technology evolves, however, it is possible that the permissioned networks utilised by financial institutions may be enhanced by the integration or interoperability of certain functionality and/or data with one or more public networks.

Each member of a permissioned network knows the identity of the counterparty on the other side of a transaction. Being able to identify a counterparty is important for many reasons in a transaction, including KYC and AML. For financial transactions, in particular, it provides parties with a way to make formal demands against each other in the event of non-performance by one of them. Similarly, if the non-performing party fails to cure a default, the other party may file a lawsuit and exercise its rights and remedies under the transaction documents. By contrast, on public networks, people are often transacting anonymously or with those who have not disclosed their true identity.

Smart contracts

The term “smart contracts” can be misleading, especially for lawyers who have a definite idea of what must be shown for there to be a binding legal agreement between parties.

At a minimum, a contract requires there to be an offer by one party, an acceptance by another party, and some form of consideration to exist. When the term is used by software engineers, it means computer code that is self-executing (the type of code will depend on the protocol on which the code is implemented). I think a more useful structure for the loan market is a hybrid legal contract that has certain parts of it coded and other parts that remain in human prose. The term “smart legal agreements” has been used to describe this type of hybrid legal contract, and this combination of a legal agreement with a smart contract would be most useful for financial instruments. One could envision how the library of LSTA’s standard forms and agreements could become smart legal agreements with certain provisions remaining in human prose; for example, the reference to LSTA Arbitration Rules in the LSTA Confirm could remain as text, while provisions relating to the calculation of the loan purchase price for the applicable trade could be coded and thus become self-executing.

There is an aspect of utilising smart legal agreements that does increase the risk of error or corruption and should, therefore, be highlighted – the management of information that is drawn from an external source referred to as an “oracle” in the blockchain nomenclature. Because smart contracts are programmed to be self-executing, some information may need to be pulled in from an external source, and therefore it is essential that this information from the oracle be accurate. For example, pursuant to the terms of the LSTA Confirm, if a trade does not timely settle, then upon settlement the buyer is credited for certain interest payments made by the borrower, but it must also pay the seller the interest that would accrue at one month LIBOR for deposits in the applicable currency as set by the ICE Benchmark Administration on the amount equal to the purchase price. If the LIBO Rate, an oracle, is corrupted for any reason, then of course there will be repercussions for trades settling on the blockchain, where the Confirm has been turned into a smart legal agreement with certain elements of it coded and thus self-executing.

Smart contracts build on the innovation of blockchain technology and have the potential to allow parties to structure and effectuate transactions in a more efficient and secure manner than traditional contracts; however, there are still challenges and obstacles that must be overcome before smart legal agreements become commonplace. Although we recognise that the technology remains in its infancy and is not a panacea for all our market’s present challenges, we remain confident that smart contracts and blockchain technology will ultimately transform our market.

Blockchain, smart contracts and the loan market

There is enormous potential for the marriage of blockchain technology and smart contracts to result in incredible strides forward for the loan market. Although the typical syndicated loan agreement is a complex instrument that cannot be reduced simply to computer code, there are aspects of it that do lend themselves to becoming coded and, where a legal agreement has been standardised for a particular market or asset, then it can be more easily coded and efficiently implemented.

In the context of the loan market, the origination of a syndicated loan – from the time the credit agreement is drafted and the loan funded – could be made using blockchain technology (as has been done in the European loan market). In today’s market, a credit agreement is typically drafted by legal counsel based on deal terms that have been emailed to them. The lawyers then prepare the draft credit documentation based on that information. This approach introduces the risk of manual transcription errors, and validation rules will not have been applied to the information included in the credit agreement. By using

document-automation tools, together with a distributed ledger, the credit agreement can be generated from data stored on the ledger that has already been validated. Although this can, of course, be accomplished without a blockchain, in the absence of one there is no single source of validated data. Having a single source of truth as to the ownership of a syndicated loan ultimately will eliminate the redundant, time-consuming, and costly exercise of multiple parties manually processing and accounting for primary allocations, payments and assignments.

In today's loan market, the closing of primary trades is a slow and time-consuming process. After initial funding of the loan by the administrative agent, each party with a primary market allocation must then fund its portion of the loan and execute an assignment agreement to evidence the settlement of their primary trade. With the disparate systems used by loan market participants today, each party is likely still emailed a PDF or another form of the executed agreement, and from those documents it must then extract the relevant information and manually input that information into its own back office system (with all the human touchpoints, there is a greater risk of error and delay with this type of process).

With a blockchain, the credit agreement and related documents could be digitally signed and delivered electronically at closing, thus allowing the deal terms, including information concerning loan positions, automatically to populate on the network's ledger – the same ledger accessed by all lenders. Think how a DLT network with the applicable credit agreement, assignment agreement and Confirm, all structured as smart legal agreements, could implement identical functionality in a way similar to today's loan operations – but one where the contracts are self-executing and the database replicated across an entire network of computers. Although the computers in the network (assuming a permissioned network is used) will be controlled by potentially hundreds of lenders in the syndicate, the integrity of the data across the network will be assured by the integration of a protocol-wide consensus mechanism.

A blockchain platform for a syndicated loan could also track a loan's interest rate, interest and principal payment dates, and any other data fields relevant to the life cycle of the loan. In a typical syndicated loan, many different parties, each storing information about a syndicated loan, have to continually reconcile all information they receive against their own internal databases. A blockchain platform could eliminate the need for, or significantly reduce the time spent on, reconciling data across the market. That alone could save the loan market an enormous amount of time and money. In addition, other aspects of a credit agreement could also be coded. For example, when a borrower submits periodic financial reports to the syndicate, certain data from those reports could be extracted, thus allowing financial covenants in the credit agreement automatically to be tested.

Secondary market trades in the loan market are memorialised by the parties executing an LSTA Confirm. Settlement of the trade – when the seller's legal ownership of the loan is transferred to the purchaser, and the purchaser pays the purchase price to the seller – typically occurs days or even weeks after the trade is entered into by the parties. It is easy to imagine how the transfer of this asset could be done far more seamlessly and efficiently on a blockchain, with smart legal agreements self-executing and data being updated on the ledger automatically. In this way, one can imagine lenders in the syndicate on a permissioned ledger using private keys digitally to execute the LSTA Confirm and applicable assignment agreements. When the assigning lender digitally signs the Confirm and relevant assignment agreement (and any other consents have been obtained), the register of lenders (assuming existing nomenclature is retained) will be updated automatically to reflect the assignee's

account being credited by the amount of the loan transferred to it, and a corresponding debit to the assignor's account. No one will need to reconcile their own positions because they will all have access on the permissioned ledger to the same information.

Although the adoption of blockchain will shorten the settlement times for loan trades, the loan purchaser must still make payment of the loan purchase price. Although it is not currently possible to transfer U.S. Dollars across a distributed ledger, there now exist a number of "stable coins", which are designed to maintain a stable relationship with the U.S. Dollar (often through reserving liquid assets). These digital assets can be exchanged for U.S. Dollars through various virtual currency exchanges. There are even a few U.S. depository institutions that have issued U.S. Dollar-equivalent digital assets. Ultimately, central bank-issued digital currency could make settlement on the blockchain seamless. A number of central banks have explored the possibility of issuing digital currency on a blockchain, and some have indicated that a limited purpose digital token for cross-border settlements may be feasible in the not so distant future. The lack of a means for making payment on a blockchain, however, can be overcome by parties continuing to use traditional payment rails to effect payment. Reliance on such external processes may be acceptable on a permissioned blockchain network, where the identities of parties are known to each other and regulated financial institutions are involved.

Last year, the LSTA completed the automation of the LSTA Form of Revolving Credit Facility. Working with OpenLaw, a blockchain-based protocol for the creation and execution of legal agreements, we used Solidity, the language native to the Ethereum platform, to code aspects of the credit agreement and create a smart legal agreement. The entire credit agreement was not turned into a smart contract; provisions relating to the mechanical aspects of the credit agreement were coded, including those relating to borrowing requests, interest and principal payments, and loan transfers. The creation of this prototype demonstrated that: (i) the drafting of syndicated credit agreements can be partly automated using legal technology tools with evidence of the parties' agreement and associated electronic signatures stored on a blockchain; (ii) smart contracts can be used to automate certain aspects of loan administration, particularly responsibilities performed by the agent; (iii) blockchain technology and smart contracts can be used to hard code regulatory compliance, in the form of approved addresses that can help ensure compliance with KYC/AML requirements (see further discussion below); (iv) blockchain technology and smart contracts can be used to hard code disqualified lender lists to help streamline the borrower consent process; and (v) blockchain technology can be used to digitally represent a lender's interest in a syndicated loan, creating opportunities to shorten settlement times for syndicated loan trades. The agreement could still be accessed, viewed, and scrolled through. Importantly, the automated contract still looked like the LSTA's credit agreement from cover page to signature page.

Unfortunately, at this time, there remain many practical limitations relating to the implementation of this new technology and smart contracts in the loan market. Because smart contracts can only interact with tokenised assets, digital assets need first to gain broader usage in our industry before blockchain-based applications and services can be widely adopted in our market. Nevertheless, we were greatly encouraged by the results of the creation of this prototype and have begun to work on automating the LSTA's Form of Investment Grade Term Sheet so that the information in that form can seamlessly flow into the automated LSTA Form of Revolving Credit Facility. We are also pleased to report that vendors focused on developing platforms for the U.S. corporate loan market are making significant progress, and we look forward to their use in the years ahead.

AML and KYC issues

An appropriately built blockchain solution for the loan market would meet both KYC and AML requirements, and in so doing, would likely improve both the speed of implementation and accuracy of a financial institution's compliance programme while satisfying any legal and regulatory requirements. The LSTA's 2018 Know Your Customer Considerations for Syndicated Lending and Loan Trading ("LSTA KYC Guidelines") serve as a comprehensive report outlining the specific due diligence and other compliance work required to engage in primary and secondary loan market transactions in the United States. The LSTA KYC Guidelines, which accurately set forth what is required for different primary and secondary loan market transactions and relationships between loan market participants, can be embedded in the smart legal agreement implementing the framework. We are pleased to report that we are currently working with U.S. regulators on "KYC Frequently Asked Questions", which are based on the LSTA's KYC Guidelines, and these FAQs once finalised will set out the KYC diligence required in the market in a straightforward question and answer format.

Because the KYC and AML requirements would be incorporated in this way, there would no longer be any need to have a separate stream of compliance work to satisfy a bank's KYC requirements and AML diligence in any syndicated loan that is processed through the framework. For example, perhaps checking the sanctions lists on the U.S. Department of the Treasury's Office of Foreign Assets Control website to ensure that a counterparty is not on any of the lists, which is typically the only due diligence required under U.S. law by an agent on a new lender, could be like an "oracle", with the diligence thereby completed seamlessly and without any delays. This would result in huge cost savings for our market and would likely also lead to much shorter loan-trade-settlement times.

Regulators would also benefit greatly from the adoption of blockchain in the loan market. Because blockchains contain a complete history of all transactions that have taken place on the network, including a time stamp for all such transactions, internal auditing would be much simpler, and regulators could be granted access to the ledger to confirm that all related transactions are consistent with the stated intentions and information provided by customers. The ability to see transactions in real time would also be beneficial to regulators, who could monitor the transactions and more easily detect and identify illicit activities.

Competition law issues and corporate governance matters

There are, of course, competition law considerations that must be taken into account when considering the implementation of this new technology, and as a trade association, whose members are often competitors of each other, we are acutely aware of these. During the process of selecting the appropriate DLT, there will be collaborative efforts necessary to implement the chosen DLT to the particular use case within the loan market. This collaboration and the development of a technological solution raise intellectual property concerns that the parties should seek to address. Although the task of identifying the correct technology may be challenging, once common ground is reached by market participants on that issue, the focus should then turn to internal governance matters, and the relative rights and obligations of the participants.

These efforts are complicated by the ever-present need to ensure compliance with applicable antitrust law, an issue that requires continuing diligence and vigilance amongst industry participants. We would caution consortium participants about antitrust issues that may arise in such circumstances, and to seek advice from counsel where appropriate. The exchange

of specific data on current and future prices and competitive activities – as opposed to aggregated past information – is likely to attract the greatest antitrust scrutiny. Thus, participants in blockchain consortia should take care to ensure that they are not, or could not be perceived to be, agreeing to eliminate their independent decision-making as to any aspect of the prices they charge or markets they serve.

Conclusion

The LSTA remains optimistic about the potential for blockchain, or any type of advanced technology, to have a positive effect on the U.S. loan market and we are pleased that, in recent years, vendors have been increasing their focus on developing advanced technological solutions for our market. At its simplest, blockchain is an efficient way to transfer any asset, including a loan, and the current systems and practices of the U.S. syndicated loan market could benefit enormously from this technology. The LSTA is well placed to lead the legal, technological, operational and business efforts to develop a general framework for implementing solutions that address the lifecycle of a loan from origination to repayment. Our market participants should understand not only the potential benefits of blockchain but the challenges to its adoption. This suggests that a sustained educational initiative targeting all loan market participants is necessary, and the LSTA is committed to offering that. The LSTA has been following developments around blockchain and providing educational resources to its members for a few years and will continue to be a resource as its members navigate many of these challenges and, in some cases, take a leading role in helping to craft standards that facilitate the efficient deployment of the technology. Forging consensus within an entire industry about standards, best practices and other uniform approaches and protocols is challenging, as we know, but the LSTA is well placed to lead these efforts.

Although blockchain technology will not eliminate all inefficiencies in the loan market, it seems very likely that blockchain technology will eventually bring about fundamental change in how syndicated loans are originated, administered and traded in today's loan market. Yet, there is much work to be done before this can be achieved. Computer software engineers, finance professionals, lawyers, and operational personnel will need to work together to analyse all of the processes used in the loan market, loan administration, and secondary loan trading. Policy, legal, and regulatory issues will need to be addressed thoughtfully, and we must always balance our desire to promote innovation with the need for a strong, stable, and reliable loan market.

**Bridget Marsh****Tel: +1 212 880 3004 / Email: bmarsh@lsta.org**

Bridget Marsh is Executive Vice President and Deputy General Counsel of the Loan Syndications and Trading Association (LSTA). Bridget heads the LSTA's Primary Market Committee and Trade Practices and Forms Committee and leads the legal projects for the development and standardisation of the LSTA's documentation.

Prior to joining the LSTA, Bridget practised as a corporate finance attorney at Milbank, New York, and as a lawyer in the corporate/M&A department of Simmons & Simmons, London, and completed a judicial clerkship for The Honorable Justice Beaumont of the Federal Court of Australia. She is a Regent of the American College of Commercial Finance Lawyers and a Fellow of the American Bar Foundation.

Bridget Marsh received a B.A. *magna cum laude* from Georgetown University, a law degree with first class honours from Sydney Law School, University of Sydney, and a Master's in Political Science from the University of New South Wales. She is admitted as an attorney in New York, England & Wales, and New South Wales, Australia.

**Josias N. Dewey****Tel: +1 305 374 8500 / Email: joe.dewey@hkllaw.com**

Joe Dewey is a financial services and real estate partner in Holland & Knight's Miami office and is considered a thought leader on blockchain technology. Mr. Dewey regularly represents banks and other financial institutions across the entire spectrum as measured by assets and scale, from community to global money center banks. Mr. Dewey spends a considerable amount of time at the convergence of human prose legal contracts, as well as computational contracts, based primarily on computer code. This includes smart contracts that can be implemented on Hyperledger Fabric (or IBM's Blockchain service), Ethereum (both public and permissioned versions) and R3's Corda platform. Mr. Dewey spends a considerable amount of his practice in this space assisting clients in identifying optimal distributed ledger use cases and developing proof of concept applications. He can assist in the transition from proof of concepts (PoCs) to production systems built by our clients' primary technology solutions providers.

Loan Syndications and Trading Association (LSTA)

366 Madison Avenue, 15th Floor, New York, NY 10017, USA
Tel: +1 212 880 3000 / Fax: +1 212 880 3040 / URL: www.lsta.org

Progress in a year of mayhem – Blockchain, cryptoassets and the evolution of global markets

Ron Quaranta
Wall Street Blockchain Alliance

There can be little doubt to readers of this current edition of the “*Global Legal Insights – Blockchain & Cryptocurrency Regulation*” publication that the year 2020 has been one of tumult and confusion. In the midst of these trying times, as nations work to recover from the human and economic tragedies of a global pandemic, as well as the political disorder that seems to be taking hold in major developed nations, it is worth noting that there has been a redoubling of efforts by some to help the advance of multiple emerging technologies. The blockchain technology and cryptoasset evolution that was previously proceeding, at least to some, in a rough and uneven manner, has become a growing wave of innovation across multiple industries and markets. The Wall Street Blockchain Alliance (WSBA) is privileged to sit beside our global members at the forefront of this evolution.

Readers of this latest edition are by now probably long familiar with the proposed benefits of blockchain technology; benefits such as decentralization, immutability and transparency, to say nothing of the as-yet-not-fully-realized cost savings possible because of these characteristics, and we will not belabor these points here. That said, the pace of actual usage and interest in blockchain technology and cryptoassets has risen. While we no longer say “this is the year that blockchain changes...” such and such industry (given how many times such change has failed to come to pass), there is no lack of noteworthy news that illustrates the growing adoption of this technology.

For example, we continue to see the evolution of the global supply chain industry leveraging blockchain technology. In arguably the most prominent example, a growing number of organizations have joined the IBM Food Trust, the most prominent being Walmart, the world’s largest company by revenue.¹ The platform is designed to increase auditability and visibility across the global food supply chain by connecting participants through a “permissioned, immutable and shared record of food provenance, transaction data, processing details, and more.”² At the time of writing, major companies including Walmart, Dole, Nestlé and more have participated in the IBM Food Trust, adding dozens of food producers, distributors, retailers and manufacturers all working to use blockchain as a permanent and shared food transactions record.

In the financial markets’ arena, a growing number of major money center banks are still testing out blockchain technology for functions like clearing and settlement, trade financing as well as other cost-prohibitive and inefficient back office processes.

Lest we think that blockchain is a disruptive force or technology for just the finance or supply chain industries, it is worth noting some of the other industries that have expressed interest. For example, airlines around the world are now beginning to look at blockchain technology for everything from inventory management to flight scheduling to passenger data management and more. In the healthcare industry, we are continuing to see an ever-

growing series of solutions designed to make the highly inefficient and very data-intensive healthcare industry more efficient, more effective and able to deliver more value to patients and doctors around the world. Patient healthcare records, which are bound by many regulations including the Health Insurance Portability and Accountability Act (or HIPAA)³ in the United States, are now being looked at as possible avenues for blockchain innovation. Given the number of data points and the challenges (as well as costs) of maintaining such records, the ability of blockchain technology to provide a clear, secure and auditable register of transactions offers an obvious solution.

Against the backdrop of these changes and evolutions of blockchain technology uses in multiple industries is the growing advancement of cryptoassets across the globe. What was once considered either an illicit invention meant to empower online criminals or to aid in tax evasion, has developed into something certainly worthy of financial markets' consideration, and a growing series of new financial instruments and all of their derivatives based on cryptoassets have evolved in the past year.

For example, the global marketplace for cryptocurrency-based derivatives is growing at an astounding pace, representing significant institutional interest in these new investment assets. In addition, derivatives based on Bitcoin or Ethereum have growing market value and growing market liquidity. Indeed, jurisdictions around the world, and the regulatory bodies that oversee them, are investing significant effort and time to make sure that these crypto derivatives are suitable and compliant for their marketplaces. The proliferation of these instruments has aroused interest in corners of the financial market that may not have seemed interested before. For example, it made news earlier in 2020 when world-famous hedge fund manager Paul Tudor Jones publicly claimed⁴ to hold several percentage points of his net worth in Bitcoin. In addition, a number of different types of financial institutions such as pension funds or family offices have also expressed interest and have now begun to educate themselves in earnest about cryptoassets and crypto derivatives. This is to say nothing of the growth of two of possibly the most prominent examples of cryptoasset evolution in the past few years, that being the rise of stablecoins as well as the rise of decentralized finance (or DeFi). It is worth addressing each of these in turn as they figure prominently in the ongoing work of the WSBA and its global member base.

Stablecoins have come to the fore in a big way in 2020. The rise of stablecoins is meant to accomplish one very specific thing, which is the minimization of volatility previously associated with most cryptocurrencies. In this context we have seen the rise of several different types of stablecoins. For example, stablecoins that are pegged to a unit of Fiat currency such as the US Dollar or the Euro. We have also seen the rise of commodity-based stablecoins that derive their value and their price based upon an underlying commodity such as oil or gold. There has also been the rise of stablecoins based on a basket of securities, which was a prominent feature of the Libra stablecoin proposed by Facebook in late 2019.⁵ In the wake of these innovations and the rise of stablecoins, industry participants are seeing ever-increasing institutional interest simply because one of the largest arguments against them participating in cryptocurrencies, namely volatility, is minimized in many instances based on stablecoin innovation. All of these developments force us to ask several interesting questions that really are at the heart of financial markets for the retail and institutional investor. How are these stablecoins valued? How can these stablecoins be traded? How and whom do we trust to be custodian for these stablecoins? These are part of the much deeper conversations that continue to occur within the WSBA membership, including the dialogues that we have in conjunction with our members as well as regulators and legislators around the world. We are beginning to see the evolution of a framework of capabilities that makes

stablecoins and cryptoassets safer, more liquid, and much more regulatorily compliant. As these developments progress, we cannot avoid the thought that cryptocurrencies and cryptoassets will continue to grow as a percentage of both institutional and retail portfolios.

Two major publications by the WSBA that we were very proud of were publications by our Accounting Working Group in cooperation with our partners and friends at AICPA⁶ and CPA.com,⁷ as well as a variety of the accounting firms that are corporately members of the WSBA. We first published our Primer on Stablecoins for the Accounting Profession, which highlighted both the definitions of stablecoins as well as the importance of understanding how stablecoins will impact the accounting profession and, by extension, the clients of accounting professionals around the world. As the use of stablecoins and the implications from a tax, regulatory and financial perspective grew, our Accounting Working Group also published a second document which was an Advanced Considerations document on stablecoins, again for the accounting professional. This document took a deeper dive into the challenges of stablecoins and really worked to help members and readers understand the challenges and importance of incorporating stablecoins into the strategy and growth of their firms. Indeed, we were very pleased when several graduate University programs in the United States requested use of the documents published by the WSBA within their graduate accounting courses, and we look forward to providing more to higher education in the future.

No less important and certainly a bit more dramatic has been the rise of DeFi.

But what exactly is DeFi? Conceptually, DeFi, what used to be called open finance, is meant to provide the same capabilities and services that we all associate with traditional financial markets. The difference is that these are meant to be provided in a decentralized way or within a decentralized framework. The digital assets and cryptoassets that we have been talking about, coupled with smart contracts and specific protocols, will empower DeFi to be built atop multiple blockchain networks. The objective of DeFi, which in the past would have been considered utopian, is the ability to give participants in the marketplace full control over their assets, providing an ecosystem without the very familiar intermediaries that we have all come to know. In addition, DeFi conceivably will allow for greater participation by the unbanked and underbanked in global financial markets. One can only imagine the benefits to individuals and the impact on poverty around the world, when people who previously did not have access to these services are finally brought into the global financial system. Interestingly, DeFi is meant to provide many of the same benefits we originally discussed in this publication three years ago, namely the benefits associated with blockchain technology. Autonomy, transparency, and tradability. The ability to engage in global financial markets' leveraging code, powered and secured by peer-to-peer technology and cryptography. Unless we think that DeFi is a passing fancy, it is worth noting that it was reported in August of 2020 that the total global value of all DeFi offerings now exceeds globally over US\$4 billion. With the rise of decentralized exchanges, greater usage and availability of stablecoins and the ability to leverage DeFi for functions like crypto lending, it is our anticipation that DeFi will be a central pillar of an evolving global financial market.

The day-to-day activities of the WSBA, in cooperation with our members, continues to expand around the world. For example, working with members of the WSBA Legal Working Group, now counting over 130 attorneys from more than 65 firms and practices around the world, the WSBA was privileged to weigh in an open commentary and requests for information from the United States Securities and Exchange Commission, the Internal Revenue Service as well as the Department of the Treasury. In the United Kingdom, we

continue to dialogue and interact with the Financial Services Authority and will continue to do so in other regions of the world, particularly Asia and Africa. Specific examples of our interactions include commentary from the WSBA Legal Working Group regarding the Office of the Comptroller of the Currency's request for information about digital payments, and how regulators should learn about and accommodate these innovations.

Our other working groups have also been very active in the global blockchain and cryptoassets marketplaces. Our Enterprise Solutions Working Group, composed of dozens of industry professionals and corporations deeply involved in the implementation of blockchain technology, has been privileged to host some of the most in-depth thought leader conversations on global enterprise adoption of blockchain anywhere in the world. Large technology companies and providers as well as small fintech and other vendors are creating new capabilities leveraging blockchain technology, and have joined us at the table with members, regulators, legislators and other innovators, to advance the cause of their industries and the strategies by which they incorporate blockchain technology and other emerging technology innovations.

Our Technology Working Group serves as the avenue by which our partnerships with global technology providers such as Hyperledger, the Linux Foundation, R3 and more, are brought forward to members. This working group has been the venue by which our members are more deeply immersed in the technical nuances of these emerging capabilities. Conversations about code, new ways of managing data, the challenges of privacy, interoperability, and integration, are all part of the ongoing discourse within this working group. The Technology Working Group shares with members and ultimately globally, not just its findings and considerations of best practices, but also the lessons learned as we focus on the emergence and usage of different types of technology within the blockchain world.

Our Cryptoassets Working Group, focused on the broad institutional adoption of cryptoassets and cryptocurrencies across the world, has spent significant time analyzing the challenges of cryptoassets, their place in global portfolios and ultimately how they might reinvent global financial markets. From hedge funds to institutional investors to banks and beyond, the Cryptoasset Working Group has played host not just to critical conversations in the world of financial markets and investment, but has also shared thought leadership amongst participants, all designed to work alongside our members and our partners and aid in the evolution of global financial markets and the benefits that that might provide.

Lastly, our recently launched Real Estate Working Group, chaired by one of the most prominent commercial real estate attorneys in the world, is focused on the broad tokenization and the token economics associated with real world assets. It is important to keep in mind that this tokenization does not just apply to commercial or even residential real estate. The tokenization of rare works of art, investment-grade wine and other hard assets that are not easily fungible nor easily traded, is a core focus of this working group. Like so many different parts of the global economy that are confronting the challenges and the opportunity of blockchain and cryptoassets, the Real Estate Working Group is focused on scholarship and important dialogue regarding such topics as the challenge of taxonomy, the task of custodianship, the management of title and ownership and many more. In addition, the challenges and impact of valuing tokenized assets is something that still needs to be developed, and our Real Estate Working Group is at the forefront of those industrywide conversations.

As we noted in the previous edition, law and regulation continue to be core components of the evolution of modern global markets. That is why the WSBA is once again very proud

to stand beside our many members and contribute to this publication, which we view as a critical guide to this fast-evolving technology. We look forward to an ongoing dialogue with our colleagues in all of the different industries involved including law, banking, trading, supply chain and beyond.

* * *

Endnotes

1. <https://en.wikipedia.org/wiki/Walmart>.
2. <https://www.ibm.com/products/food-trust>.
3. https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act.
4. <https://www.cnbc.com/2020/05/11/paul-tudor-jones-calls-bitcoin-a-great-speculation-says-he-has-almost-2percent-of-his-assets-in-it.html>.
5. [https://en.wikipedia.org/wiki/Libra_\(digital_currency\)](https://en.wikipedia.org/wiki/Libra_(digital_currency)).
6. <https://www.aicpa.org>.
7. <https://www.cpa.com>.

* * *

Information about the Wall Street Blockchain Alliance can be found at www.wsba.co, or by email to info@wsba.co.

**Ron Quaranta****Email: ron@wsba.co**

Ron possesses over three decades of experience in the global financial services and technology industries. He currently serves as Chairman and Chief Executive Officer of the Wall Street Blockchain Alliance, the world's leading non-profit trade association promoting the comprehensive adoption of blockchain technology and cryptoassets across global markets. Prior to this, Ron served as Chief Executive Officer of DerivaTrust Technologies, a pioneering software and technology firm for financial market participants. Ron is the editor and contributing author of the book "*Blockchain in Financial Markets and Beyond: Challenges and Applications*", published by Risk Books, as well as a contributor to "*GLI – Blockchain & Cryptocurrency Regulation 2020*", published by Global Legal Group. He was named in the Top 100 Most Influential People in Accounting by *Accounting Today* in 2018 and is the lead author for the ISACA Blockchain Framework as well as a member of the ISACA Emerging Technology Advisory Group. He is a frequent guest of major media outlets, including Bloomberg Radio, and is a sought-after speaker and writer regarding financial technology and innovation. Ron also serves as an advisor to multiple startups and corporations focused on fintech innovation and blockchain technology.

Wall Street Blockchain Alliance

Email: info@wsba.coURL: www.wsba.co

Cryptocurrency and blockchain in the 116th Congress

Jason Brett & Whitney Kalmbach
Value Technology Foundation¹

The 116th United States Congress – in session from January 3, 2019 to January 3, 2021 – has seen an influx of cryptocurrency and blockchain bills introduced in both the House of Representatives and the Senate. As rapid cryptocurrency and blockchain innovations require changes in the lexicology on a frequent basis, this Congress introduced legislation addressing “stablecoins” as well as “digital dollars”² or U.S. central bank digital currency (“CBDC”). Between January 2019 through the end of August 2020, there were 36 pieces of legislation that we have broken down into four main policy areas: (1) addressing the use of cryptocurrency by terrorists, money launderers, and human and sex traffickers; (2) creating a regulatory framework for blockchain and cryptocurrencies; (3) promoting U.S. Government use of blockchain technology; and (4) establishing a U.S. CBDC or digital U.S. dollar.³

In early 2019, the United States faced the prospect of Venezuela, led by the dictatorship of Nicolás Maduro, creating its own digital currency as a way to circumvent U.S. economic sanctions. Along with the rising problems of worldwide human and sex trafficking, legislators also focused on how virtual currencies might play a role in this area. Additionally, concerns of money laundering and terrorist fundraising through cryptocurrencies held the focus of many in Congress. These drove what amounts to one-third, or 12, of the 36 bills that were introduced by Congress.

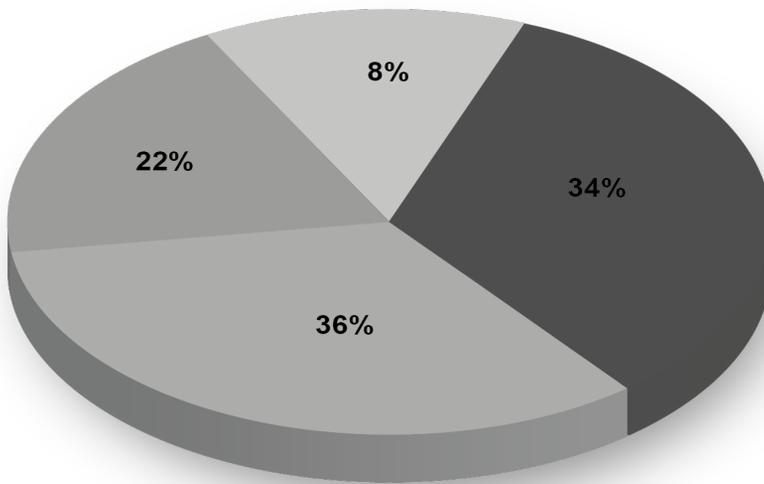
In mid-2019, Facebook’s introduction of Project Libra⁴ created a real-world scenario that forced Congress to evaluate the policy implications of cryptocurrencies and blockchain. The potential for mass adoption among Facebook’s 2.7 billion users became a concern as to its competition against U.S. fiat currency. The notion of “stablecoins”, or a way to provide cryptocurrency with a relatively stable value to address volatility risks, caught the attention of Facebook as a way to achieve this type of mass adoption.⁵ Additionally, U.S. financial technology (or “FinTech”) companies and U.S. policymakers showed a growing interest in the digital payment offerings of Chinese companies, WeChat and Alipay,⁶ to users of their social media apps, with increasing numbers of such users funding and using these apps as a “store of value” for their money. Combined with a handful of legislators from the Congressional Blockchain Caucus⁷ that are actively exploring ways to improve the legal and regulatory environment for cryptocurrency and blockchain technology, a total of 13 bills were introduced that focused on creating a framework for the regulation of cryptocurrency and blockchain in the United States.

Besides a natural focus on the illicit uses of cryptocurrency and the establishment of regulations for a blockchain-based economy, bills also addressed how the U.S. Government itself may benefit from the technology. Eight bills either focused on the development of blockchain technology or included parts that aimed at helping the U.S. Government better understand and explore ways of using the technology.

As Project Libra seemed to accelerate the possibility of China launching its own digital currency,⁸ the COVID-19 pandemic further accelerated the trend toward digital currency in Asia. Legislators also were looking for innovative ways of distributing stimulus payments through digital dollars. This new concept of “digital dollars”, or a U.S. CBDC, was introduced in three different bills in the 116th Congress.

The chart below shows the percentage that fall into each of the four main policy areas identified by the Value Technology Foundation of all the cryptocurrency and blockchain bills that have been introduced in the 116th Congress from January 2019 through the end of August 2020. After the chart, a detailed discussion of all 36 bills introduced so far by category is provided in this chapter.

Crypto and Blockchain Legislation in the 116th Congress 2019–2020



- Use of Cryptocurrency in Potential Terrorism, Money Laundering, and Human and Sex Trafficking (34%)
- Regulatory Framework and Treatment of Cryptocurrency and Blockchain (36%)
- Promoting the Use of Blockchain by the U.S. Government (22%)
- U.S. Central Bank Digital Currency and Digital Dollar (8%)

Source: Value Technology Foundation

Use of cryptocurrency by terrorists, money launderers, and human/sex traffickers

This section analyses the 12 bills that address policies around the ways cryptocurrency may be used by terrorists, money launderers, and human/sex traffickers.

Sub-Policy Areas	No. of Bills	Bill Names
Addressing Cryptocurrency Use for Evasion of U.S. Sanctions	2	VERDAD Act; and Further Consolidated Appropriations Act of 2020
Addressing Cryptocurrency Use for Human/Sex Trafficking	4	FIND Act; End Banking for Human Trafficking Act; EARN IT Act; and ILLICIT CASH Act

Sub-Policy Areas	No. of Bills	Bill Names
Cryptocurrency Use by Terrorists/ Money Launderers	3	Financial Technology Protection Act; Homeland Security Assessment Act; and FinCEN Improvement Act
Exploring Blockchain Technology Use by Law Enforcement/Bank Examiners	3	COUNTER Act; Advancing Innovation to Assist Law Enforcement Act; and Corporate Transparency Act
Exploring Protection of Cryptocurrency Exchanges from Hacks	1	Defending American Security from Kremlin Aggression Act of 2019

Sub-Policy Area: Addressing Cryptocurrency Use for Evasion of U.S. Sanctions

VERDAD Act

The VERDAD (or the Venezuela Emergency Relief, Democracy Assistance, and Development) Act of 2019 (S. 1025)⁹ directs the President to take various actions to address the political situation in Venezuela. This bill is motivated by the fact that the United States does not recognise Nicolás Maduro as Venezuela’s President due to reports of widespread fraud during his election, recognising instead National Assembly President Juan Guaidó.

The bill creates “cryptocurrency sanctions” as a means of enforcing the effectiveness of U.S. sanctions. Maduro launched a cryptocurrency in 2018 called the “Petro” which is backed by the country’s oil. The stated purpose of the Petro¹⁰ was to circumvent the sanctions of the United States in attempting to force a regime change in Venezuela.

The bill was introduced as a way to support Executive Order 13827,¹¹ signed on March 19, 2018, which prohibits transactions by a U.S. person or within the United States that relate to, provide financing for, or otherwise deal in any digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Maduro regime. Such transactions are prohibited beginning on the date of the enactment of this Act.

As of August 2020, the bill has been voted out of the Committee on Foreign Relations and awaits a vote by the full U.S. Senate. With 18 co-sponsors, the bill represents almost 20% of the entire Senate in terms of sponsorship, which is the highest representation of any cryptocurrency or blockchain bill of Senators or Members of Congress.

Notably, there is a related House bill, H.R. 1865,¹² that under Subtitle G – “Cryptocurrency and Ensuring the Effectiveness of United States Sanctions”, the bill would require the Secretary of State and the Secretary of the Treasury, after consultation with the Chairman of the Securities and Exchange Commission (“SEC”) and the Chairman of the Commodity Futures Trading Commission (“CFTC”), to develop a methodology to assess how any Maduro regime-issued digital currency, digital coin, or digital token is being used to circumvent or undermine U.S. sanctions.

The authors wish to point out that the concept of a foreign country “printing” its own electronic form of money and being able to transact in cryptocurrencies with other countries in theory provides an easy way for countries to avoid sanctions imposed by the United States. As sanctions are an integral part of the U.S. Government’s foreign policy toolkit, the prospect of other countries creating their own digital currency threatens the enforcement of U.S. sanctions and represents a risk that the Department of the Treasury and Department of State are closely monitoring. Although the Petro was never a truly functioning cryptocurrency, the concept also sparked a request in the VERDAD Act for a briefing on the overall impact of cryptocurrencies on U.S. sanctions.

Sub-Policy Area: Addressing Cryptocurrency Use for Human/Sex Trafficking

The FIND Trafficking Act

H.R. 502 or the FIND (Fight Illicit Networks and Detect) Trafficking Act¹³ directs the Government Accountability Office (“GAO”) to report on the use of virtual currencies and online marketplaces in sex and drug trafficking. It requires the Comptroller General to carry out a study on how virtual currencies and online marketplaces are used to buy, sell, or facilitate the financing of goods or services associated with sex trafficking or drug trafficking, and for other purposes. The GAO is required to study topics including how illicit proceeds are transferred into the U.S. banking system, which State and non-State actors participate in such activity, and what kind of preventative efforts Federal and State agencies are taking.

Additionally, the FIND Trafficking Act directs the GAO to study the extent to which the unique characteristics of virtual currencies can contribute to the tracking and prosecution of illicit funding. The bill has passed the House of Representatives and is in the Senate, currently in the Committee on Banking, Housing, and Urban Affairs as of August 2020.

End Banking for Human Traffickers Act of 2019

The End Banking for Human Traffickers Act of 2019, or H.R. 295,¹⁴ provides a means to recommend changes, if necessary, to existing statutory law to more effectively detect and deter money laundering relating to severe forms of trafficking in persons, where such money laundering involves the use of emerging technologies and virtual currencies.

The Interagency Task Force to Monitor and Combat Trafficking¹⁵ would provide appropriate legislative, administrative, and other recommendations to Congress after completing an analysis. As of August 2020, the bill was voted out of Committee and awaits a vote in the House of Representatives.

EARN IT Act

The Eliminating Abusive and Rampant Neglect of Interactive Technologies, known as the “EARN IT Act” (S. 398),¹⁶ establishes a National Commission on Online Child Sexual Exploitation Prevention to develop recommended best practices that providers of interactive computer services may choose to implement to prevent, reduce, and respond to the online sexual exploitation of children.

The EARN IT Act was widely seen by such organisations as the Electronic Frontier Foundation¹⁷ as violating the Constitutional right of free speech by requiring companies to adopt a list of best practices issued from the Attorney General’s Office. Many believe that Congress should not selectively grant Section 230 immunity only to online platforms that comply with best practices that interfere with their First Amendment right to make editorial choices regarding their hosting of user-generated content. The bill also threatens to provide the Government with a “backdoor” into end-to-end encryption tools as a way of effectively enforcing the EARN IT Act, which raises obvious privacy concerns and presents challenges to the future development of blockchain technology.

In that the EARN IT Act threatens Section 230 immunity, which is needed for nascent blockchain platforms to grow without undue legal risk, and the inability to use end-to-end encryption, it therefore creates critical problems for the growth of blockchain technology in the United States. It also impacts a portion of the crypto community who are particularly committed to supporting online privacy rights.

As of August 2020, the EARN IT Act was voted out of Committee and awaits a vote by the Senate.

ILLICIT CASH Act

Under the Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings Act, or the ILLICIT CASH Act (S. 2563),¹⁸ the Comptroller General of the United States, head of the GAO, is required to conduct a study on how virtual currencies and online marketplaces are used to facilitate human and drug trafficking. The goal of this portion of the bill is to improve money laundering enforcement, similar to the FIND Act.

Sub-Policy Area: Policy Addressing Cryptocurrency Use by Terrorists/Money Launderers *Financial Technology Protection Act*

The Financial Technology Protection Act, or H.R. 56,¹⁹ provides for the investigation of new financial technologies (e.g., digital currencies) and their use in terrorism and other illicit activities. The bill establishes an Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing to research terrorist and illicit use of new financial technologies and to issue an annual report.

This bill also empowers the Department of the Treasury to provide a reward for any person who provides information leading to the conviction of an individual involved with terrorist use of digital currencies. The Secretary of the Treasury, in consultation with the Attorney General, must establish a fund to pay a reward, not to exceed \$450,000, to any person who provides information leading to the conviction of an individual involved with terrorist use of digital currencies.

Additionally, the bill establishes a FinTech Leadership in Innovation and Financial Intelligence Program to support the development of tools and programmes to detect terrorist and illicit use of digital currencies. The Secretary of the Treasury may make grants to entities located in the United States, including academic institutions, companies, non-profit institutions, individuals, and any other entities located in the United States that the Secretary determines appropriate.

As of August 2020, this bill has passed the House of Representatives, and is currently in the Senate Banking Committee. Besides requiring an annual report issued by this new Task Force, the bill is unique in also offering both rewards and grant money.

Homeland Security Assessment of Terrorists' Use of Virtual Currencies Act

The Homeland Security Assessment of Terrorists' Use of Virtual Currencies Act²⁰ directs the Department of Homeland Security's Office of Intelligence and Analysis to assess the threat posed by individuals using virtual currencies to support terrorism. The assessment must be shared with State, Tribal and local law enforcement officials.

The Office of Intelligence and Analysis is required to develop and disseminate a threat assessment regarding the actual and potential threat posed by individuals using virtual currency to carry out activities in furtherance of an act of terrorism, including the provision of material support or resources to a foreign terrorist organisation. This bill passed the House of Representatives and is currently in the Senate Committee on Homeland Security and Governmental Affairs.

In August 2020, the Department of Justice made an arrest that involved the largest seizure ever of cryptocurrency accounts,²¹ showing that crypto is a tool for terrorist activity. Law enforcement authorities are observing and acting on this trend.

FinCEN Improvement Act

The FinCEN Improvement Act, or H.R. 1414,²² strengthens the Financial Crimes Enforcement Network ("FinCEN") to include matters involving emerging technologies or

value that substitutes for currency. Although the use and trading of virtual currencies are legal practices, some terrorists and criminals, including international criminal organisations, seek to exploit vulnerabilities in the global financial system and are increasingly using emerging payment methods such as virtual currencies to move illicit funds. Since September 11, 2001, the Federal Bureau of Investigation (“FBI”) has reported that the threat landscape in general for terrorists has expanded.

As of August 2020, H.R. 1414 passed the House of Representatives – a companion bill had also been introduced to the Senate (S. 582).²³

Sub-Policy Area: Exploring Blockchain Technology Use by Law Enforcement/Bank Examiners

On the flip side of looking to stop or thwart attempts by terrorists to use virtual currencies to launder money or fund their operations, is the technology of blockchain itself which could offer insights into who and where the virtual currencies are transferred to. In three bills – the COUNTER Act, the Advancing Innovation to Assist Law Enforcement Act, and the Corporate Transparency Act – there is language requiring the FinCEN to analyse how it could better use artificial intelligence (“AI”), digital identity technologies, and blockchain technology to more actively analyse and disseminate the information it collects and stores to provide investigative leads to Federal, State, Tribal and local law enforcement.

COUNTER Act

The COUNTER (Coordinating Oversight, Upgrading and Innovating Technology, and Examiner Reform) Act of 2019, or H.R. 2514,²⁴ has passed the House and is currently in the Senate. The COUNTER Act asks the Director of FinCEN to carry out a study that examines the status of implementation and internal use of emerging technologies, including AI, digital identity technologies, blockchain technologies, and other innovative technologies within FinCEN. The COUNTER Act examines whether these innovative technologies can be further leveraged to make FinCEN’s data analysis more efficient and effective.

The COUNTER Act also asks FinCEN to study how it could better use these innovative technologies to more actively analyse and disseminate the information it collects and stores to provide investigative leads to Federal, State, Tribal, and local law enforcement, and other Federal agencies. As of August 2020, the bill passed the House of Representatives and is in the Senate.

Advancing Innovation to Assist Law Enforcement Act

The Advancing Innovation to Assist Law Enforcement Act, or H.R. 2613,²⁵ has passed the House and is currently in the Senate Banking Committee. The exact language in H.R. 2613 is also in the COUNTER Act, as described above. As of August 2020, this bill passed the House of Representatives and is in the Senate as well.

Corporate Transparency Act

The Corporate Transparency Act, or H.R. 2513,²⁶ requires that certain new and existing small corporations and limited liability companies disclose information about their beneficial owners. A beneficial owner is an individual who (1) exercises substantial control over a corporation or limited liability company, (2) owns 25% or more of the interest in a corporation or limited liability company, or (3) receives substantial economic benefits from the assets of a corporation or limited liability company.

The bill contains the same language as in H.R. 2613 and H.R. 2514 above, with the same request for FinCEN to conduct a study, as described above. As of August 2020, the Corporate Transparency Act has also passed the House of Representatives and is in the Senate.

Sub-Policy Area: Exploring Protection of Cryptocurrency Exchanges from Hacks

Defending American Security from Kremlin Aggression Act of 2019

The Defending American Security from Kremlin Aggression Act of 2019 (S. 482)²⁷ seeks to promote international efforts to protect financial institutions and cryptocurrency exchanges from cyber theft. The bill establishes the Office of Cyberspace and the Digital Economy to assess ways to protect America from cybersecurity attacks into banks and cryptocurrency exchanges.

The bill is significant in that it designates both banks and cryptocurrency exchanges as essential financial services organisations that could provide the Russians with a tremendous amount of money, an outcome that is seen as needing to be avoided for the national security of the United States. This is the only bill that affords cryptocurrency exchanges similar protections to those that financial institutions enjoy. As of August 2020, the bill is out of Committee and waiting for a vote by the full Senate.

Regulatory clarity for cryptocurrency and blockchain companies

Sub-Policy Areas	No. of Bills	Bill Names
Addressing Blockchain Token Treatment for Businesses	4	Token Taxonomy Act; Digital Taxonomy Act; U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2019; and Crypto-Currency Act of 2020
Addressing Consumer Protection	2	Virtual Currency Consumer Protection Act; and Bill to amend the CEA on regulation of virtual currencies
Addressing State Money Transmission Licences	1	Blockchain Regulatory Certainty Act
Addressing Taxation of Blockchain Tokens	3	Safe Harbor for Taxpayers with Forked Assets Act; Virtual Value Tax Fit Act of 2019; and Virtual Currency Tax Fairness Act
Addressing Facebook's Libra Coin	3	Managed Stablecoins are Securities; Keep Big Tech Out of Finance; and Protecting Consumers from Market Manipulation Act

Sub-Policy Area: Addressing Blockchain Token Treatment for Businesses

Token Taxonomy Act

The Token Taxonomy Act²⁸ would have a direct impact as to how digital tokens will be regulated and by which agency. The bill would amend the Securities Act of 1933 and the Securities Exchange Act of 1934 to exclude digital tokens from the definition of a security. The bill directs the SEC to enact certain regulatory changes regarding digital units secured through public key cryptography. Moreover, this bill preempts States' rights requiring, or with respect to, registration or qualification of securities.

The Token Taxonomy Act would also adjust the taxation of virtual currencies held in individual retirement accounts to create a tax exemption for exchanges of one virtual currency for another and create a *de minimis* exemption from taxation for gains realised from the sale or exchange of virtual currency for cash.

Because the Token Taxonomy Act focuses on both an amendment to the Securities Act of 1933 and the Securities Exchange Act of 1934, the bill has been referred to both the House Financial Services Committee and the Ways and Means Committee. As of August 2020, the bill is still in the House of Representatives.

Digital Taxonomy Act

The Digital Taxonomy Act²⁹ is a bill that requires the Federal Trade Commission ("FTC") to develop a plan for preventing unfair or deceptive practices relating to transactions involving

digital tokens, including any recommendations for further action by Congress. It was designed as a companion bill to the Token Taxonomy Act, above. In the definition of the bill, digital tokens include digital currency or cryptocurrency.

This bill would give the FTC \$25,000,000 a year for five fiscal years to prevent unfair and deceptive practices in transactions relating to digital tokens. The FTC is to provide a report and legislative recommendations to Congress. In the report, the FTC should offer a plan to prevent unfair or deceptive acts or practices relating to digital tokens. The report would also provide recommendations for legislation that would improve the ability of the FTC and other relevant Federal agencies to further protect consumers from unfair or deceptive acts or practices in the digital token marketplace, promote the competitiveness of the United States, and promote innovation of businesses in the global digital token marketplace. As of August 2020, the bill is in Committee in the House of Representatives.

U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2019

The U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2019, or H.R. 923,³⁰ seeks to promote U.S. competitiveness in the evolving global virtual currency marketplace. Given that virtual currency could have a significant effect on the economy, regulation of virtual currency may be important to protect investors, deter bad actors, create market certainty, and ensure American competitiveness in an evolving global marketplace.

This bill requires the CFTC Chair and the SEC Chair, along with other relevant agencies, to prepare a report on the state of virtual markets and ways to promote American competitiveness. The report is to include the regulation of the U.S. virtual currency industry as a comparative study relative to the regulation of such industry in foreign countries to demonstrate the competitiveness in a global marketplace and the potential benefits of virtual currency and blockchain technology in the U.S. commodities market.

The report would also analyse the current regulatory environment in the United States, make legislative suggestions, and clarify which virtual currencies qualify as commodities for both existing currencies and ones that may be created in the future. It would also provide a new, optional regulatory structure for virtual currency spot markets (commonly referred to as exchanges) that includes Federal licensure, market supervision, consumer protections, and preemption of State money transmission licensing obligations for participating in spot markets. As of August 2020, the bill is in Committee in the House of Representatives.

Crypto-Currency Act of 2020

Introduced on March 9, 2020, the Crypto-Currency Act of 2020, or H.R. 6154,³¹ offers a broad approach on how to regulate the cryptocurrency industry and categorise digital assets. The purpose of the bill is to clarify which Federal agencies regulate digital assets, and to require those agencies to notify the public of any Federal licences, certifications, or registrations required to create or trade in such assets. This approach, with a focus on the economic behaviours of the underlying digital instruments, was also recommended in a report³² by the Federal Reserve Bank of Dallas.

The Secretary of the Treasury, acting through the FinCEN, and the Comptroller of the Currency (“OCC”) would be the designated primary Government agencies with the authority to regulate cryptocurrencies (other than synthetic stablecoins). The bill designates the SEC as the primary Government agency with the authority to regulate crypto-securities and synthetic stablecoins. The CFTC would be the primary Government agency with the authority to regulate crypto-commodities. For cryptocurrencies, reserve-backed stablecoins that are representations of a U.S. or foreign country’s currency, and collateralised on a one-

to-one basis by such currency, would be regulated by FinCEN and the OCC. Synthetic stablecoins, which the bill defines as any digital asset, other than reserve-backed stablecoins, that are stabilised against the value of a currency or other asset, and rest on a blockchain or decentralised cryptographic ledger, would be regulated by the SEC.

As of August 2020, H.R. 6154 is in the House Committee on Financial Services and the House Agriculture Committee.

Sub-Policy Area: Addressing Consumer Protection

Virtual Currency Consumer Protection Act of 2019

The Virtual Currency Consumer Protection Act of 2019³³ was introduced to promote fair and transparent virtual currency markets by examining the potential for price manipulation. The bill calls for a study and report by the Chairs of the CFTC and SEC on the prevention of virtual currency price manipulation.

The report is to cover methods by which persons could manipulate the price of virtual currencies, which types of virtual currency, if any, are more susceptible to being manipulated, and the effects on, and particular harm to, investors if price manipulation of virtual currencies occurs. As of August 2020, the bill was in Committee in the House.

Bill to amend the CEA on regulation of virtual currencies

A bill to amend the Commodities Exchange Act (“CEA”), or H.R. 4234,³⁴ would strengthen the CFTC’s role in regulating digital commodities, such as Bitcoin (or crypto-based derivatives). The bill passed out of the House Agriculture Committee. The bill has a provision which was added to the CFTC Reauthorization Act of 2019 to offer unconstrained access to all trade and trader data regarding the virtual currency on the spot market platform and the capability to provide the data to the CFTC on request.

On March 11, 2020, the associated H.R. 6197³⁵ to reauthorise the CFTC was referred to the House Committee on Agriculture.

Sub-Policy Area: Addressing State Money Transmission Licences

Blockchain Regulatory Certainty Act

The Blockchain Regulatory Certainty Act, or H.R. 528,³⁶ offers protection for non-controlling blockchain services providers and software developers. No blockchain developer or provider of a blockchain service shall be treated as a money transmitter, financial institution, or any other State or Federal legal designation requiring licensing or registration as a condition to acting as a blockchain developer or provider of a blockchain service, unless the developer or provider has, in the regular course of business, control over digital currency to which a user is entitled under the blockchain service or the software created, maintained, or disseminated by the blockchain developer.

Essentially, the bill provides a safe harbour from licensing and registration for certain non-controlling blockchain developers and providers of blockchain services.

As of August 2020, after introduction in the House, the bill was last referred to the House Subcommittee on Courts, Intellectual Property, and the Internet, and has not progressed further.

Sub-Policy Area: Addressing Taxation of Blockchain Tokens

Safe Harbor for Taxpayers with Forked Assets Act of 2019

The Safe Harbor for Taxpayers with Forked Assets Act of 2019³⁷ provides a temporary safe harbour on forked assets in the absence of Internal Revenue Service (“IRS”) guidance. The safe harbour covers the tax treatment of hard forks of convertible virtual currency in the absence of administrative guidance.

This bill was introduced as a means to offer a temporary solution for taxpayers and also as a way of urging the IRS to devise guidance and a framework that taxpayers could follow to handle the taxation on forked assets. As of August 2020, the bill was introduced in the House and was in Committee.

Virtual Value Tax Fit Act of 2019

The Virtual Value Tax Fit Act of 2019³⁸ would amend the Internal Revenue Code of 1986 to allow exclusion of gain or loss on like-kind exchanges of virtual currency. The exchange of virtual currency for virtual currency of like kind is to be treated in the same manner as the exchange of real property for real property of like kind.

As of August 2020, the Virtual Value Tax Fit Act of 2019 had been introduced in the House and in the Ways and Means Committee.

Virtual Currency Tax Fairness Act

The Virtual Currency Tax Fairness Act³⁹ amends the Internal Revenue Code of 1986 to exclude gross income gain from disposition of virtual currency in a personal transaction with an exception for transactions up to \$200. As of August 2020, the Virtual Currency Tax Fairness Act was introduced in the House and in the Ways and Means Committee.

Sub-Policy Area: Addressing Facebook’s Libra Cryptocurrency and Blockchain

Three bills were introduced as a direct result of and in response to Facebook’s announcement of Project Libra. The bills were extremely prescriptive in nature with aims as direct as keeping a company like Facebook out of the financial sector as always. The three bills are analysed and described below.

Managed Stablecoins are Securities Act

The Managed Stablecoins are Securities Act⁴⁰ was created as a way to establish the treatment of managed stablecoins under the securities laws. This piece of legislation would protect consumers against certain cryptocurrencies, such as the Facebook Libra Project. The bill would clarify that “managed stablecoins” are securities under the Securities Exchange Act of 1934 and are thus regulated by the SEC. As of August 2020, the bill was introduced in the House of Representatives and referred to the House Financial Services Committee.

This was the first of three bills that were created as a result of Facebook Libra which, with its initial concept of having its “Libra Coin” backed by a basket of currencies, would limit its use in payments by designating it as a security.

Keep Big Tech Out of Finance Act

The Keep Big Tech Out of Finance Act⁴¹ prohibits large platform utilities from being a financial institution or being affiliated with a person that is a financial institution. A large platform utility may not be, and may not be affiliated with any person that is, a financial institution. According to the bill, a large platform utility may not establish, maintain, or operate a digital asset that is intended to be widely used as a medium of exchange, unit of account, store of value, or any other similar function, as defined by the Board of Governors of the Federal Reserve System.

Any large platform utility or financial institution that violates the bill shall be subject to a fine of not more than \$1,000,000 per each day of such violation, in an action brought by the appropriate Federal financial regulator. A large platform utility means a technology company with an annual global revenue of \$25,000,000,000 or more, and that is predominantly engaged in the business of offering to the public an online marketplace, an exchange, or a platform for connecting third parties.

For any large platform utility with a cryptocurrency prior to the enactment of this law, the platform utility would have one year to remove its cryptocurrency offering. This was the second of three bills that targeted Facebook, with this being the most direct – and the most prescriptive – legislation that would ban Facebook and other large social media platforms from engaging in the financial sector. As of August 2020, the bill had been introduced to the House and referred to the Financial Services Committee.

Protecting Consumers from Market Manipulation Act

The Protecting Consumers from Market Manipulation Act⁴² amends the Bank Holding Company Act of 1956 to restore the separation between banking and commerce by prohibiting bank holding company ownership of non-financial assets. The bill directs that a large non-financial company that is not registered as a bank holding company may not (either directly or indirectly, or through a subsidiary) engage in activities that are financial in nature if engaging in such activities would result in such activities producing the lower of (1) 5% of the revenue of the large non-financial company, or (2) \$1,000,000,000 in revenue. A large non-financial company is defined in the bill as having annual revenues of more than \$5,000,000,000 and is not predominantly engaged in financial activities.

The bill also calls for two reports to be prepared. First, the Financial Stability Oversight Council (“FSOC”) would be required to carry out a study and issue a report to Congress that examines the financial stability implications of digital currency and also determines whether digital currencies should be designated as designated financial market utilities under Title VIII of the Payment, Clearing, and Settlement Supervision Act of 2010. Second, the bill calls for a Federal Reserve Study that examines the monetary policy and monetary sovereignty implications of digital currency and proposes a framework for supervising any digital currency that is designated as a designated financial market utility under Title VIII of the Payment, Clearing, and Settlement Supervision Act of 2010. This is the only consumer protection bill that focuses on FSOC and the Federal Reserve to provide reports covering the systemic risk implications of cryptocurrencies. As of August 2020, the bill was introduced in the House and is in the Financial Services Committee.

In looking to separate “banking” from “commerce”, the bill would force any “non-financial firm”, such as a Facebook as an example, to register as a bank holding company, which is a company that holds interests in one or more banks but does not engage in banking activities itself. This third bill also seeks to place digital currencies as “designated financial market utilities”, which means that because of their level of use in commerce, an evaluation of whether there are systemic risks to the financial system needs to be incorporated in the regulatory regime. Between the Managed Stablecoins are Securities Act, the Keep Big Tech Out of Finance Act, and the Protecting Consumers from Market Manipulation Act, the broad implications of what Facebook posed was essentially opposed by designating the Libra cryptocurrency as a security, blocking Facebook from engaging in finance at all, and asserting that should Facebook own a company or subsidiary that engages in banking, based on certain amounts, that Facebook would be forced to stop conducting business in Libra or seek a bank holding company charter from the Federal Reserve.

Use of blockchain technology in Government

Sub-Policy Areas	No. of Bills	Bill Names
Exploring Blockchain Promotion Across All U.S. Government Agencies	2	Blockchain Promotion Act; and Advancing Blockchain Act
Exploring Blockchain for Hospital Data Security for Endemic Fungal Disease Research	1	FORWARD Act

Sub-Policy Areas	No. of Bills	Bill Names
Exploring a Blockchain Study in Export-Import Bank on Supply Chain for Exporters	1	U.S. Export Finance Agency Act
Exploring Blockchain for Increasing Investments by Lower-Income Individuals	1	Rescue Act for Black and Community Banks
Mandating Blockchain Use for Supplies of Personal Protective Equipment in the United States	1	Strategic National Stockpile Enhancement and Transparency Act
Exploring Blockchain for Use by the Department of Defense	1	National Defense Authorization Act of 2020

Sub-Policy Area: Exploring Blockchain Promotion Across All U.S. Government Agencies

Blockchain Promotion Act

The Blockchain Promotion Act (S. 553)⁴³ passed out of Committee and created a Working Group that would provide a definition of blockchain to Congress. The bill also asks for a report on the blockchain use for electromagnetic spectrum with the Federal Communications Commission (“FCC”). The idea would be to focus on blockchain use in other areas besides crypto in the U.S. Government. The companion legislation from the House of Representatives, H.R. 1361, is still in the original Committee to which the bill was referred, while the Senate version of the bill awaits a vote from the upper chamber.

Advancing Blockchain Act

The Advancing Blockchain Act⁴⁴ requires the Secretary of Commerce and the FTC to conduct a study on blockchain technology, and for other purposes. This bill seems markedly similar to the original Blockchain Promotion Act; however, this bill was unilaterally introduced in connection with a number of bills by the Republican side in the Energy and Commerce Committee.⁴⁵

This bill notably lacked a bipartisan approach for the first time – which is an exception to the rule of how almost all the blockchain and cryptocurrency bills up to this point had been forged in the spirit of bipartisanship, or at least avoided any “partisan” undertones. As of August 2020, the bill is in the House of Representatives in the Energy and Commerce Committee.

Sub-Policy Area: Exploring Blockchain for Hospital Data Security for Endemic Fungal Disease Research

FORWARD Act of 2019

The FORWARD Act of 2019,⁴⁶ or Finding Orphan-disease Remedies with Antifungal Research and Development Act of 2019, will support endemic fungal disease research, incentivise fungal vaccine development, discover new antifungal therapies and diagnostics, and for other purposes. The bill specifically implements a blockchain pilot programme for hospital data security for endemic fungal disease research. The bill is in the Energy and Commerce Committee in the House as of August 2020.

Sub-Policy Area: Exploring a Blockchain Study in Export-Import Bank on Supply Chain for Exporters

United States Export Finance Agency Act of 2019

The United States Export Finance Agency Act of 2019⁴⁷ provides for a general study by the Export Finance Agency, including policy recommendations on development, use, and security of blockchain in operations of U.S. exporters. The survey would be carried out by the President of the U.S. Export Finance Agency, with State exporters benefitting from Agency support regarding the use of blockchain in their operations, including their

management of supply chains, contracts, and payments. The survey would involve an assessment of the effects of blockchain on reliability, transparency, and security in the operations. There would also be policy recommendations to improve the development, use, and security of blockchain in the operations of U.S. exporters.

An updated bill, H.R. 4863,⁴⁸ was ultimately introduced without this survey requirement, and contained other changes to major parts of the bill as a result of bipartisan efforts that proved unsuccessful. With these updates, H.R. 4863 passed the House and is in the Senate.

As described earlier, H.R. 1865,⁴⁹ which cared for how Congress determined appropriations that law became law, contains a related provision in Title IV, Export-Import Bank Extension, Section 402: Program on China and Transformational Exports. This provision would require the Bank to establish a Program on China and Transformational Exports to enhance U.S. competitiveness. One of the stated objectives of the Program is to “advance the comparative leadership of the United States with respect to the People’s Republic of China, or support United States innovation, employment, and technological standards, through direct exports” in AI, wireless communications equipment (including 5G or subsequent wireless technologies), and emerging financial technologies that facilitate financial inclusion, data security and privacy, payments, the transfer of funds, and associated messaging services, and efforts to combat money laundering and the financing of terrorism. Cryptocurrency and blockchain and distributed ledger technologies (“DLTs”) could potentially fall within the scope of this provision. Of note, the Value Technology Foundation is addressing the issue of U.S. competitiveness relative to China in the realm of DLTs in an upcoming paper.⁵⁰

Sub-Policy Area: Exploring Blockchain for Increasing Investments by Lower-Income Individuals

Rescue Act for Black and Community Banks

The Rescue Act for Black and Community Banks, or H.R. 41,⁵¹ requires the GAO to study the use of the new markets tax credit, lower-value home mortgages, and blockchain investments. The bill requires the Comptroller General of the United States to carry out a study on blockchain technology and whether such technology could be used to increase investment by lower-income individuals in startups and other crowdfunded companies. As of August 2020, the bill is in the House of Representatives in the Financial Services Committee and the Ways and Means Committee.

Sub-Policy Area: Mandating Blockchain Use for Monitoring Supplies of Personal Protective Equipment in the United States

Strategic National Stockpile Enhancement and Transparency Act

The Strategic National Stockpile Enhancement and Transparency Act⁵² directs the Secretary of Health and Human Services (“HHS”) to establish, in coordination with the Director of the Strategic National Stockpile, the National Emergency Biodefense Network. This bill requires the Department of HHS to establish and award grants to States for the implementation of the National Emergency Biodefense Network.

HHS must coordinate with the Strategic National Stockpile and the National Biodefense Science Board in this effort. The network consists of State entities responsible for tracking and maintaining adequate supplies of drugs, medical devices, and other items necessary for the emergency health security of the United States. The network must be developed and implemented using a private blockchain, as opposed to a permissionless Bitcoin or Ethereum network.

While this bill was introduced in response to the COVID-19 pandemic, it is intended to address the Nation's PPE supply for a 2021 or 2022 timeframe, in the event of a future pandemic. As of August 2020, the bill is in the House of Representatives in the Energy and Commerce Committee.

Sub-Policy Area: Exploring Blockchain Use by the Department of Defense

National Defense Authorization Act of 2020

The National Defense Authorization Act of 2020 contained a provision (S. 255) that would require the Under Secretary of Defense for Research and Engineering to provide, no later than 180 days after the enactment of this Act, to the Congressional defence committees a briefing on the potential use of DLT for defence purposes. This provision is in the final report⁵³ and not in the bill, but has the effect of law. The Senate bill contained no similar provision; however, as it did not object to the inclusion of the Amendment in the House, the requirement of a briefing carries the same effect as the bill passed into law.

The report directs the Under Secretary of Defense for Research and Engineering to provide, no later than 180 days after the date of the enactment of this Act, to the congressional defence committees a briefing on the potential use of DLT for defence purposes. This briefing shall include an explanation of how DLT may be used by the Department of Defense to: (1) improve cybersecurity, beginning at the hardware level, of vulnerable assets such as energy, water, and transport grids through distributed *versus* centralised computing; (2) reduce single points of failure in emergency and catastrophe decision-making by subjecting decisions to consensus validation through DLTs; (3) improve the efficiency of defence logistics and supply chain operations; (4) enhance the transparency of procurement auditing; and (5) allow innovations to be adapted by the private sector for ancillary uses. The briefing is also to include any other information that the Under Secretary of Defense for Research and Engineering determines to be appropriate.

As of August 2020, the bill had been passed into law; however, details of the required briefing that may have been classified have not yet been released by the U.S. Government.

Policy focusing on U.S. central bank digital currencies

Sub-Policy Area	No. of Bills	Bill Names
Policy Focusing on U.S. Central Bank Digital Currencies	3	Banking for All Act; Automatic BOOST to Communities Act; and Financial Protections and Assistance for America's Consumers, States, Businesses, and Vulnerable Populations Act

Sub-Policy Area: Policy Focusing on U.S. Central Bank Digital Currencies

Banking for All Act

The Banking for All Act (S. 3571)⁵⁴ requires member banks to maintain pass-through digital dollar wallets for certain persons, and for other purposes. The bill establishes digital dollar wallets that are to be maintained at member banks for COVID-19 payments. The bill would also create postal retail facilities as an extension of the Federal Reserve System, as well as digital dollar wallets. State non-member banks or credit unions will be entitled to reimbursement. Under the regulation of the Federal Reserve, Pass-Through FedAccounts would not be subject to any account fees, minimum balances, or maximum balances and would pay interest at a rate not below the greater of the rate of interest on required reserves and the rate of interest on excess reserves.

The authors observe that the fundamental motivation of this bill was the compelling need to deliver stimulus payments to Americans during the COVID-19 pandemic. The bill also advances the principle that everyone deserves a free bank account that makes their money available to them in a timely manner. As of August 2020, the bill was introduced in the Senate and is in the Senate Banking Committee.

Automatic BOOST to Communities Act

The Automatic BOOST to Communities (“ABC Act”)⁵⁵ directs the Secretary of the Treasury to establish the BOOST Communities Program to provide monthly payments to America’s consumers during the COVID-19 pandemic to recover from the emergency, and for other purposes.

The ABC Act immediately provides a \$2,000 payment using BOOST debit cards to every person in America as critical relief during the COVID-19 crisis, followed by \$1,000 recurring monthly payments for one year after the end of the crisis to help families recover. The ABC Act would be funded directly from the Treasury with no additional debt issued by minting two \$1 trillion coins, and additional trillion-dollar coins as necessary. The creation of these platinum coins at the Treasury is also a symbolic representation in policy that demonstrates how the Treasury should be addressing fiscal policy, while the Federal Reserve should only be addressing monetary policy.

As this bill relates to the “digital dollar”, the bill calls for the creation of a digital dollar and a digital dollar wallet, with the concept being that a digital dollar wallet should be provided to the American people through the U.S. Treasury, with a digital dollar being implemented by the Federal Reserve. The bill requires that stimulus payments be made in digital dollars to holders of digital dollar wallets for those who wish to opt in to receiving payments as such. As of August 2020, the bill was introduced in the House and is in the House Financial Services Committee.

Financial Protections and Assistance for America’s Consumers, States, Businesses, and Vulnerable Populations Act

The Financial Protections and Assistance for America’s Consumers, States, Businesses, and Vulnerable Populations Act, or H.R. 6321,⁵⁶ was introduced as a separate bill during the time of the Coronavirus Aid, Relief, and Economic Security (“CARES”) Act that provides for the first, and as of this writing, the only, round of direct stimulus payments to the American people.

The bill would have provided payments to individuals of up to \$2,000 a month, subject to limits based on adjusted gross income and established digital wallets for individuals without bank accounts to receive such payments. It also, for the first time in a bill, fully and directly expressed a definition of a digital dollar. The bill would define the term “digital dollar” as a balance expressed as a dollar value consisting of digital ledger entries that are recorded as liabilities in the accounts of any Federal Reserve bank; or an electronic unit of value, redeemable by an eligible financial institution (as determined by the Board of Governors of the Federal Reserve System).

The amount of payments the bill offers for a qualified individual age 18 or older is \$2,000. For any qualified individual under age 18, the amount is \$1,000. Ultimately, this concept was not included in the CARES Act and it is highly unlikely that it will move forward. As of August 2020, the bill is in the House of Representatives in the Financial Services Committee.

Conclusion

The 116th Congress paid significant attention to blockchain and cryptocurrencies, as demonstrated by the 36 bills reviewed in this chapter. The authors view this attention as a positive sign that Congress is well aware of the pressing need for legislators and regulators to understand and embrace the growing global use of cryptocurrencies and blockchain technologies, while ensuring that the United States deploys these emerging technologies in responsible and beneficial ways to preserve and protect America's interests and public policies.

* * *

Endnotes

1. The Value Technology Foundation (“VTF”) is a 501(c)(3) non-profit think tank based in Washington, D.C. VTF focuses on blockchain and distributed ledger technologies, advocating and providing policy prescriptions for legislators and regulators for the advancement of these technologies in the United States and in other open, free societies. Jason Brett is the Chief Executive Officer of VTF and Whitney Kalmbach is VTF’s Chief Operating Officer. The authors wish to acknowledge the editorial contributions of Laura Harper Powell, Esq., VTF’s former Senior Legal Fellow, and Geetika Jerath, Esq., an Associate of Norton Rose Fulbright US LLP.
2. <https://www.wsj.com/articles/we-sent-a-man-to-the-moon-we-can-send-the-dollar-to-cyberspace-11571179923>.
3. VTF’s process in determining the number of bills related to blockchain and cryptocurrency is based on the activity publicly disclosed on <https://www.congress.gov> as of the time of writing and categories are assigned based on the general types of issues addressed by each bill.
4. <https://libra.org/en-US/>.
5. <https://techcrunch.com/2018/12/21/facebook-stablecoin/>.
6. <https://www.businessinsider.com/alipay-wechat-pay-china-mobile-payments-street-vendors-musicians-2018-5>.
7. <https://congressionalblockchaincaucus-schweikert.house.gov/members>.
8. <https://www.coindesk.com/digital-currency-china-central-bank-yuan-tests>.
9. <https://www.congress.gov/116/bills/s1025/BILLS-116s1025rs.pdf>.
10. <https://www.nytimes.com/2017/12/03/world/americas/venezuela-cryptocurrency-maduro.html>.
11. <https://thefederalregister.org/83-FR/12469/2018-05916.pdf>.
12. <https://www.congress.gov/116/bills/hr1865/BILLS-116hr1865enr.pdf>.
13. <https://www.congress.gov/116/bills/hr502/BILLS-116hr502rfs.pdf>.
14. <https://www.congress.gov/116/bills/hr295/BILLS-116hr295ih.pdf>.
15. <https://www.state.gov/the-presidents-interagency-task-force/#:~:text=The%20President%20Interagency%20Task%20Force%20to%20Monitor%20and%20Combat%20Trafficking,government%2Dwide%20efforts%20to%20combat>.
16. <https://www.congress.gov/bill/116th-congress/senate-bill/3398?q=%7B%22search%22%3A%5B%22earn+it%22%5D%7D&s=4&r=2>.
17. <https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution>.
18. <https://www.congress.gov/116/bills/s2563/BILLS-116s2563is.pdf>.
19. <https://www.congress.gov/116/bills/hr56/BILLS-116hr56rfs.pdf>.
20. <https://www.congress.gov/116/bills/hr428/BILLS-116hr428eh.pdf>.

21. <https://www.justice.gov/usao-nj/pr/three-men-arrested-722-million-cryptocurrency-fraud-scheme>.
22. <https://www.congress.gov/116/bills/hr1414/BILLS-116hr1414rfs.pdf>.
23. <https://www.congress.gov/116/bills/s582/BILLS-116s582is.pdf>.
24. <https://www.congress.gov/116/bills/hr2514/BILLS-116hr2514rfs.pdf>.
25. <https://www.congress.gov/116/bills/hr2613/BILLS-116hr2613rfs.pdf>.
26. <https://www.congress.gov/116/bills/hr2513/BILLS-116hr2513rfs.pdf>.
27. <https://www.congress.gov/116/bills/s482/BILLS-116s482rs.pdf>.
28. <https://www.congress.gov/116/bills/hr2144/BILLS-116hr2144ih.pdf>.
29. <https://www.congress.gov/116/bills/hr2154/BILLS-116hr2154ih.pdf>.
30. <https://www.congress.gov/116/bills/hr923/BILLS-116hr923ih.pdf>.
31. <https://www.congress.gov/116/bills/hr6154/BILLS-116hr6154ih.pdf>.
32. <https://www.dallasfed.org/institute/wpapers/2020/0381>.
33. <https://www.congress.gov/116/bills/hr922/BILLS-116hr922ih.pdf>.
34. <https://www.congress.gov/116/bills/hr4234/BILLS-116hr4234ih.pdf>.
35. <https://www.congress.gov/116/bills/hr6197/BILLS-116hr6197ih.pdf>.
36. <https://www.congress.gov/116/bills/hr528/BILLS-116hr528ih.pdf>.
37. <https://www.congress.gov/116/bills/hr3650/BILLS-116hr3650ih.pdf>.
38. <https://www.congress.gov/116/bills/hr3963/BILLS-116hr3963ih.pdf>.
39. <https://www.congress.gov/116/bills/hr5635/BILLS-116hr5635ih.pdf>.
40. <https://www.congress.gov/116/bills/hr5197/BILLS-116hr5197ih.pdf>.
41. <https://www.congress.gov/116/bills/hr4813/BILLS-116hr4813ih.pdf>.
42. <https://www.congress.gov/116/bills/hr5180/BILLS-116hr5180ih.pdf>.
43. <https://www.congress.gov/116/bills/s553/BILLS-116s553rs.pdf>.
44. <https://www.congress.gov/116/bills/hr6938/BILLS-116hr6938ih.pdf>.
45. <https://republicans-energycommerce.house.gov/news/press-release/walden-mcmorris-rodriguez-announce-emerging-tech-agenda/>.
46. <https://www.congress.gov/116/bills/hr2858/BILLS-116hr2858ih.pdf>.
47. <https://www.congress.gov/116/bills/hr3407/BILLS-116hr3407ih.pdf>.
48. <https://www.congress.gov/116/bills/hr4863/BILLS-116hr4863rfs.pdf>.
49. <https://www.congress.gov/116/bills/hr1865/BILLS-116hr1865enr.pdf>.
50. Please visit <https://www.valuetechology.org> to download this paper.
51. <https://www.congress.gov/116/bills/hr41/BILLS-116hr41ih.pdf>.
52. <https://www.congress.gov/116/bills/hr6607/BILLS-116hr6607ih.pdf>.
53. <https://www.congress.gov/116/crpt/hrpt333/CRPT-116hrpt333.pdf>.
54. <https://www.congress.gov/116/bills/s3571/BILLS-116s3571is.pdf>.
55. <https://www.congress.gov/116/bills/hr6553/BILLS-116hr6553ih.pdf>.
56. <https://www.congress.gov/116/bills/hr6321/BILLS-116hr6321ih.pdf>.

**Jason Brett****Tel: +1 703 215 5213 / Email: jason@valuetechology.org**

Jason Brett formerly served as a regulator at the FDIC during the last financial crisis. Additionally, he has extensive experience in developing and implementing successful governmental affairs programmes for various companies, including clients of Key Bridge Advisors. While serving as Policy Director for the blockchain technology company ConsenSys, he was responsible for their domestic and international policy during a key period of their growth. Jason has also worked as a consultant at Booz Allen Hamilton, and the Operations Director for the Digital Chamber of Commerce. He is the Founder and CEO of the Value Technology Foundation, a non-profit technology think tank. He is also a forbes.com contributor who writes on policy issues related to cryptocurrency and blockchain. Jason holds an M.B.A. from American University and a Bachelor's degree from Cornell University.

**Whitney Kalmbach****Tel: +1 703 215 5213 / Email: whitney@valuetechology.org**

Whitney Kalmbach is a former U.S. Naval Intelligence Officer with experience working in financial services, military contracting, business development, and consulting at JPMorgan Chase, Raytheon, and Deloitte. At Raytheon, she worked on the Corporate Strategy team which is responsible for developing the overarching strategies for the company, including the Five-Year Plan and Acquisition Strategy. At Deloitte, she was responsible for helping to plan and execute key U.S. Navy systems consolidations. Her consulting work has helped clients pursue valuable business development opportunities. She can provide clients extensive business planning and financial modelling expertise. She has also been instrumental in launching and growing the operations of the Value Technology Foundation, a non-profit technology think tank. Whitney holds an Executive M.B.A. from the Wharton School, University of Pennsylvania, and a Bachelor's degree from Princeton University.

Value Technology Foundation

1101 Wilson Blvd Floor 6, Office 952, Arlington, VA 22209, USA

Tel: +1 703 215 5213 / URL: www.valuetechology.org

Blockchain and intellectual property: A case study

Joshua Krumholz, Ieuan G. Mahony & Brian J. Colandreo
Holland & Knight LLP

Introduction

As discussed elsewhere in this book, blockchain has the potential for transformational change. Like most transformational technologies, its development and adoption is laden with intellectual property (“IP”) issues, concerns and strategies. Further, given the potentially wide-ranging impact of blockchain technology, the public and private nature of its application, and the prevalent use of open source software, blockchain raises particularly unique IP issues.

The purpose of this chapter is to help the practitioner identify some of the issues that may affect blockchain development and adoption. We address these issues as they may relate to a company’s creation of its own IP, and as they may relate to efforts by others to assert their IP against a company. We discuss the issues in the context of the hypothetical scenario discussed below.

The hypothetical transaction

Although many sectors stand to benefit from the use of blockchain technology, the financial and supply chain management sectors may be among the first to benefit. For purposes of discussion, this chapter focuses on the financial sector, and in particular the following hypothetical:

A U.S. company is building a new platform using distributed ledger technology for its syndicated loan transactions. Many participants are involved in a typical transaction serviced by the platform, including borrowers, lenders, an administrative agent, credit enhancers and holders of subordinated debt. The platform that the company is building employs smart contracts to effectuate the functionality over a permissioned (private) network with several hundred nodes in the network.

Our hypothetical company, as noted, has chosen to deploy its solution via a permissioned network. A blockchain developer has two broad options in this regard. First, the developer could select a public blockchain network for its platform. In a public network, each node contains all transactions, the nodes are anonymous, and participants are unknown to each other. Second, the developer could select a permissioned network (as our hypothetical company has). In a permissioned network, the network owner vets network members, accepts only those that it trusts, and uses an access control layer to prevent others from accessing the network. Unlike the nodes on a public network, the nodes on a permissioned network are not anonymous. In addition, a permissioned network can be structured so that specified transactions and data reside only on identified nodes, and are not stored on all nodes in the network.¹ In certain commercial transactions, participants must be known to each other in order to meet regulatory requirements, such as those designed to prevent money laundering. In these situations, a network of anonymous nodes would not be compliant.

Our hypothetical company has selected a permissioned network, we can assume, to obtain these benefits. This selection comes with costs, however, and the company will lose the benefit, for example, of validating a transaction over the full multitude of distributed nodes in a public blockchain network, and the assurances of immutability that this provides.

The blockchain patent landscape

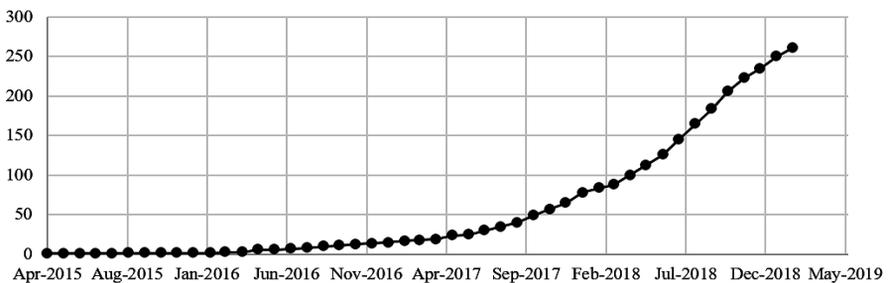
Since Satoshi Nakamoto published the Bitcoin whitepaper in 2008,^{2,3} the number of worldwide blockchain patent applications has steadily risen:

Year	Patent Application Filings (Worldwide)
2016 ⁴	895
2017 ⁵	1,631
2018 ⁶	4,673
2019 ⁷	5,800

Notably, two Chinese entities (Tencent and Alibaba Group) filed the greatest number of blockchain patent applications in 2019, accounting for 20% of all filed applications.⁸ The top four entities that filed for a blockchain patent in 2019 were all based in China.⁹

The number of issued U.S. patents has likewise risen over time. In 2015, the United States issued only two patents relating to blockchain. In 2018, there were 170 such patents. As of mid-2019, that figure had risen to 260. The chart below depicts the rapid growth of U.S. blockchain patents:

Blockchain Patents Issued Over Time [Monthly Cumulative]



The largest holders of these U.S. blockchain patents as of mid-2019 are shown below:¹⁰

Entity	Industry	No. of Blockchain Patents
IBM	Technology	57
Accenture	Technology	26
Bank of America	Finance	24
Mastercard	Finance	13
Winklevoss IP	IP holding	13
Capital One	Finance	10
Vijay Madisetti	Academic	9
TD Bank	Finance	9
Dell	Technology	9
Blockchain ASICs	IP holding	7

Because blockchain technology assists in the efficient and secure transfer of assets, it is no surprise that the financial industry currently dominates the blockchain patent space. Technology companies like IBM¹¹ and Dell¹² also are utilizing blockchains to improve existing technologies and processes, including supply chain and digital rights management. The IP holding companies, meanwhile, presumably seek patents solely to monetize them.

What can be protected?

Only new and novel ideas may be patented

Ideas that already are in the public domain may not be patented, and much of blockchain technology falls into that category. As discussed elsewhere in this book, a blockchain is a distributed ledgering system that allows for the memorializing of transactions in a manner that is not easily counterfeited, is self-authenticating, and is inherently secure. The basic concept of a blockchain may not be patented. A ledgering system that records such transactions, employs multiple identical copies of the ledgers, and maintains them in separate and distinct entities, similarly may not be patented as a new and novel idea. Blockchain technology also uses cryptography. Known cryptography techniques, even if used for the first time with blockchain, also are not likely to be patentable unless the combination resulted from unique insights or efforts to overcome unique technical problems.

Anyone is generally free to use these concepts and, as such, they are not patentable. So what is left that can be protected? Only novel and non-obvious ways to use the above-described blockchain distributed ledger system may be protected. For example, the traditional banking industry utilizes central banks and clearing houses to effectuate the transfer of money between entities, which often results in significant delay to complete the transactions. With access to overnight shipping, real-time, chat-based customer service, and social networks allowing for the live video conferencing of multiple parties positioned around the globe, it is understandable that today's consumer could be disillusioned with the pace at which financial transactions move through the traditional banking industry.

Accordingly, various companies and entities are devoting considerable time and resources to refining and revising the manner in which the traditional banking industry effectuates such monetary transactions. Entrepreneurial companies are inventing unique systems for effectuating asset transfers between banking entities that are memorialized via the above-described blockchain distributed ledgering system, as well as unique systems for expanding the utility of distributed ledgers via remote (and cryptographically secured) content defined within the distributed ledgers. These improvements, as a general proposition, build and improve upon the foundational blockchain technology. Such an improvement could take the form, for example, of an application deployed on the "foundation" of the Hyperledger platform and designed to verify the identity of participants in the hypothetical company's permissioned network, or to create audit trails for transactions on this network. It is these incremental improvements that potentially may be patentable. And it is in this area that our hypothetical company should be focusing its patenting efforts.

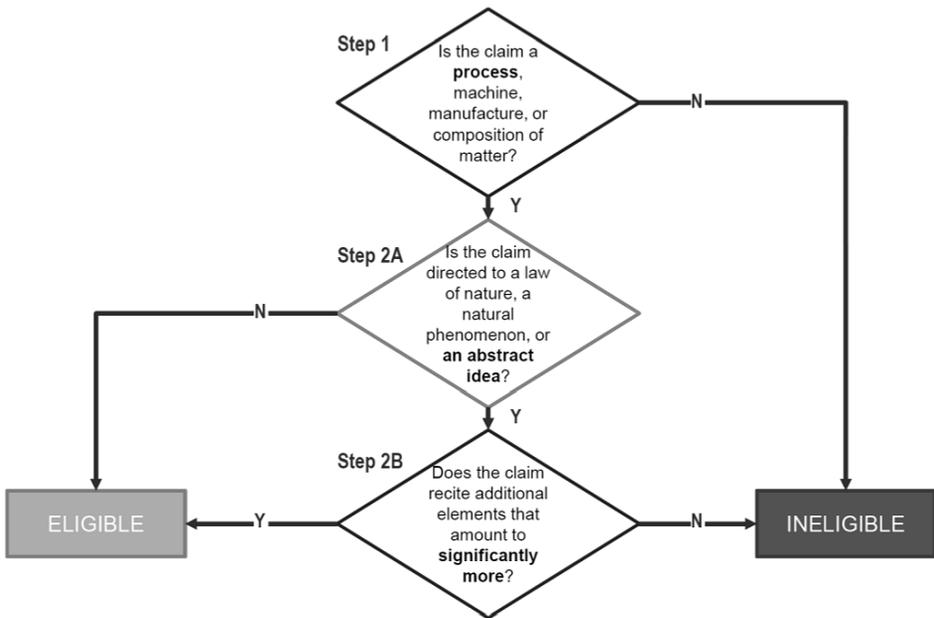
The Alice decision

Obtaining a patent by our hypothetical company also faces another obstacle. As explained by the Supreme Court in *Alice Corp. v. CLS Bank Int'l*, to be patentable, a claimed invention must be something more than just an abstract idea.¹³ Rather, it

must involve a technical solution to a specific problem or limitation in the field. In the *Alice* case, for example, a computer system was used as a third-party intermediary between parties to an exchange, wherein the intermediary created “shadow” credit and debit records (*i.e.*, account ledgers) that mirrored the balances in the parties’ real-world accounts at “exchange institutions” (*e.g.*, banks). The intermediary updated the shadow records in real time as transactions were entered, thus allowing only those transactions for which the parties’ updated shadow records indicated sufficient resources to satisfy their mutual obligations.

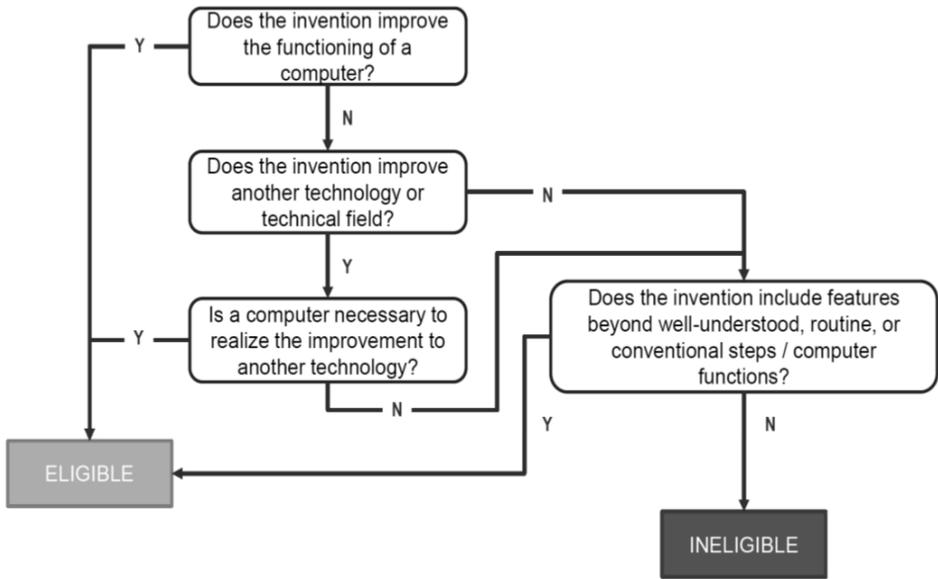
The Supreme Court held that, “on their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk.” The Court went on to explain that “the concept of intermediated settlement is a fundamental economic practice long prevalent in our system of commerce.” The Court then explained that such basic economic principles could not be patented, even if implemented in software or in some other concrete manner, because abstract ideas are not themselves patentable. Allowing patents on abstract ideas themselves, the Supreme Court explained, would significantly restrict and dampen innovation.

The following flowchart defines the manner in which the patentability of subject matter should be analyzed with respect to the *Alice* decision:



As such, basic concepts, even as they relate to blockchain, may not be patentable. So our hypothetical company must present more than just basic, economic principles in order to get a patent. It must, for example, claim specific improvements to the functioning of a computer, improvements to other, related technology, effect a transformation of a particular article to a different state or thing, add a specific implementation that is not well understood, routine or conventional, or add unconventional steps that confine the claim to a particular useful application.

The following flowchart may be utilized when assessing the patentability of subject matter with respect to the *Alice* decision:



If the *Alice* decision taught practitioners anything, it is that IP law is continuously changing. Accordingly, just as a sound investment plan requires a diversified securities portfolio, a sound IP strategy requires a diversified IP portfolio. Therefore, companies should not put all of their proverbial eggs into one IP basket. For example, if a company was in the “intermediated settlement” space and all they owned were U.S. utility patents, the *Alice* decision would have been devastating to it.

Accordingly, companies should include utility patents in their IP portfolio. But the prudent company also would include: design patents (for protecting, *e.g.*, user interfaces); trade secrets (for protecting, *e.g.*, backend algorithms that are not susceptible to reverse engineering); trademarks (for protecting the goodwill associated with the products produced by the company); service marks (for protecting the goodwill associated with the services provided by the company); copyrights (for protecting software code, and/or the expression of a concept or an idea); and various IP agreements (*e.g.*, employment agreements, development agreements, and licensing agreements). The best IP portfolio for our hypothetical company, therefore, should resemble a quilt that is constructed of various discrete components (utility patents, design patents, trade secrets, trademarks, service marks, copyrights, and IP agreements) that are combined to provide the desired level of IP coverage.

The assertion and defense of patent litigation

The threat of patent litigation

Just a few years ago, patent litigation was ubiquitous. Identifying a unique market opportunity, non-practicing entities (“NPEs”), also known as “patent trolls,” sprung up, aggregated patents, targeted specific industries, and monetized those patents either through threats of litigation or actual lawsuits. One sector that was the subject of this attack was the telecommunications industry. Beyond a number of competitor *versus* competitor suits (such as *Apple v. Samsung*), large, sophisticated NPEs also arose that did not make a product or

sell a service. Rather, they purchased patents, created portfolios, and engaged in litigation campaigns to force companies to pay royalties on those patents. Often, if an NPE had a large enough portfolio, then a company would enter into a license agreement to license that portfolio for a defined period of time, often five years.

In the last few years, patent litigation has waned. Due to Congress's creation of *inter partes* review ("IPR") proceedings, stricter requirements on proving damages, member organizations that acquire patents and offer licenses to their members, restrictions on where patent lawsuits may be filed, and new defenses that more easily allow patents to be invalidated at the early stages of litigation, patent litigation is no longer the economic opportunity that it previously had been. While competitors still will engage in patent litigation to preserve (or attack) their relative positions in the marketplace, NPEs have found that this changing landscape has made patent litigation financially less rewarding. To be sure, such patent litigation still exists. Indeed, new lawsuits are filed daily. The number and threat of those lawsuits has greatly diminished, however, and the value of patents generally has diminished as well.

Market changes, of course, can create new incentives for initiating patent litigations, and the increased role of blockchain technology is likely to bring about one of those changes. To the extent blockchain technology becomes prevalent, it is likely to result in substantially increased patent litigation, both between competitors and between NPEs and practicing companies. The reasons for this potential change are several:

- In a competitive landscape, certain companies—specifically those technology companies solely directed toward creating blockchain products—must use their patents to keep competitors out of the marketplace.
- Blockchain is ushering in a new set of patents, based on new technology, that have not been licensed.
- Blockchain technology will be used in lucrative fields which, by association, will make blockchain patents more valuable.
- Blockchain technology likely will be used as fundamental building blocks, making the technology more valuable and damages more lucrative.
- Blockchain startups that hold patents may fail, which could put those patents in the hands of an NPE.

Certainly, NPEs see the opportunity. Erich Spangenberg, a well-known founder of NPEs, has set up IPwe to collect and exploit blockchain patents, and Intellectual Ventures, a well-known and well-financed NPE, similarly is seeking to acquire and exploit patents in this area.¹⁴ And our hypothetical transaction platform reflects this opportunity. If our hypothetical company builds blockchain technology into the basic building blocks of its transactions, and its transactions form the basic building blocks of its business, then it stands to reason that the technology underlying those activities has significant value.

Offensive and defensive uses of patent rights

When entering into this new technical field, therefore, it is critical that our hypothetical company understands the patent landscape. Are there so many patents that they create a barrier to entry? Are other companies actively applying for patents? If so, are they doing so to block others or require licensing fees, or are they doing so merely for defensive purposes? Understanding and properly predicting this landscape may be the difference between a successful and a failed endeavor.

Broadly speaking, the strategic use of patent rights can be categorized as offensive or defensive (or a mix of the two). These strategies are discussed in greater detail below.

Offensive uses of patent rights

From an offensive perspective, the holder of a patent gains the right to exclude others from making, using or selling the invention.¹⁵ An offensive patent holder therefore has the ability to block all others from utilizing its patented inventions. In an emerging technical field like blockchain, patent filers typically have a more open landscape of new solutions to discover and claim. Because of the patent holder's right to exclude, each solution it is able to patent can block competitors from utilizing that solution in their own products or services absent permission.

For our hypothetical company, if the patented technology allows for a more efficient and secure transaction, then our hypothetical company may want to exclude others from using that technology, giving the hypothetical company a competitive advantage in the marketplace. If our hypothetical company does not wish to exclude competitors, it may instead allow other companies to use its patented technology, but demand that they pay reasonable royalties for that use, perhaps to help defray research and development costs or to create an alternative revenue stream.

It is not enough, however, for the offensive patent holder to file and receive issued patents. The offensive patent holder must affirmatively enforce its patent rights, and make sure that those patent rights are not encumbered by open source licenses, per our discussion in the section "The impact of open source software" below, or by FRAND licensing obligations, per our discussion in the section "The role of industry standards" below. Enforcement requires monitoring for activities that may infringe the patent holder's claims, demanding that others halt infringing activities and, if necessary, instituting litigation to halt the activities by and/or receive reasonable compensation for those activities.

Our hypothetical company also may seek to develop income streams from its patent portfolio. By enforcing its patent rights, the offensive patent holder may force competitors to take and pay for licenses. These licenses may provide income to the offensive patent holder as a single lump sum, where the licensee pays for its license upfront, or as a running royalty, where the licensee pays a percentage of the revenue generated by its products in the marketplace.

Defensive uses of patent rights

Rather than affirmatively asserting patents, the defensive patent holder uses them as a hedge against other potential claims against it. Thus, if the hypothetical company is building a platform and cannot have that platform's use interrupted, then the hypothetical company needs to build up as many defenses against a claim of patent infringement as possible. By having its own portfolio, our hypothetical company may be able to deter competitors from a lawsuit against it, because that competitor knows that it may face claims against it if it brings a patent infringement action.

A defensive strategy, if timely performed, also can block others from securing patents that later can be asserted against it. That is, in fact, the precise strategy of Coinbase's patent filings. By filing for as many patents as possible in the blockchain field, Coinbase hopes to take away patent rights from NPEs, which those entities could otherwise assert against Coinbase.¹⁶

Ultimately, as blockchain matures, players in the field will tend to take several forms. Patent leaders will emerge, and to avoid mutual destruction, they will enter into cross-licenses with each other. Other companies will try to enter the industry without a proper patent portfolio, and may find significant barriers to entry if the existing patent leaders seek to assert their right to exclude those other companies from using their patented technology. And then

there will be companies that simply acquire patents for the purpose of asserting them. Such companies will create transaction costs but should not bar entry into the marketplace.

* * *

Our hypothetical company must then consider a long-term strategy. Is it creating a platform of critical importance, but leaving itself vulnerable to its competitors? Is it fully taking advantage of its hard work and innovation by protecting the original and novel concepts that it created? Will it find itself blocked by aggressive competitors that are aggregating important patents? All of these questions must be addressed at the same time that our hypothetical company is investing in its technological improvements, and seeking to attract entities and (perhaps) developers to join and participate in its newly created blockchain network.

Strategies for limiting patent litigation exposure

The threat of patent litigation in the blockchain field is real. So how can our hypothetical company limit potential liability? There are several steps that it can take:

- **Open source defenses.** At a minimum, if a claim is asserted, our hypothetical company needs to consider whether that claim is blocked or barred by open source restrictions. In addition, our company also should be deliberating carefully on its own open source strategy, and how the use of open source software impacts its potential defenses and assertion rights.
- **Actively enter into cross-license agreements.** If our hypothetical company has acquired a significant patent portfolio, then it may want to approach other major players in the blockchain field and seek to enter into cross-licenses with those companies. This approach allows companies to compete based on the quality of their product or service, rather than engage in a damaging patent war.
- **Join patent pools.** In certain industries, particularly telecommunications, patent pools have arisen to help combat NPEs. These patent pools are membership-based organizations, whereby companies pay a fee for a license to all patents held by the pool. The patent pool's typical approach is to acquire patents, or take licenses on patents, for the benefit of its members. The goal of these organizations is to charge a reasonable fee for a license to a broad-based portfolio.
- **Monitoring patent application and allowed patents.** While there are many blockchain patents and patent applications, they number in the hundreds, not the thousands. As such, if committed, our hypothetical company can review patent applications as they are published (18 months after filing) and when patents issue (on average 3–4 years after filing). Doing so allows a company to identify potentially problematic patents. The downside of such an approach, however, is that such monitoring may become discoverable in a patent litigation, and perhaps can be used as evidence of knowing (willful) infringement.
- **Consider design arounds where available.** To the extent our hypothetical company identifies potentially problematic patents or applications, an option for it is to “design around” the problematic patent. In other words, our hypothetical company can analyze the particular elements that make up the invention, and eliminate one or more of those elements in its product in order to avoid practicing the patent.
- **Be prepared to file IPRs.** If our hypothetical company finds a problematic patent, then one option is to file an IPR with the Patent Office to try to invalidate the patent. Our hypothetical company can take that step even if no lawsuit has been filed against it. Deciding whether to do so requires an assessment of the likelihood that the patent can be invalidated and the cost associated with that process, but that cost will always be substantially less than the cost of patent litigation.

- **Be prepared to attack the patents on *Alice* grounds.** If our hypothetical company ends up in litigation, it still may be able to terminate that litigation early by filing an *Alice* motion, discussed more fully in the section “Offensive and defensive uses of patent rights” above. The blockchain concept itself is an abstract idea, and not patentable as such. To have a valid blockchain patent, the claimed idea must identify some technical problem in the field and provide some specific technical solution to that problem. Without providing something sufficiently concrete, our hypothetical company may be able to invalidate the asserted patent early in the litigation process.
- **Assert counterclaims.** As discussed above, it is important for our hypothetical company to acquire its own patent portfolio. If successful in doing that, and if sued by a practicing company, then our hypothetical company may be able to assert its own claims of patent infringement. Doing so typically makes it easier to resolve a dispute in its early stages.

The impact of open source software

The term “open source software” refers to software that is distributed in source code form. In source code form, the software can be tested, modified, and improved by entities other than the original developer. The term “proprietary” software refers to software that, in contrast, is distributed in object code form only. The developer of proprietary software protects its source code as a trade secret, and declines to allow others to modify, maintain, or have visibility into its software code base. Proponents of open source software state that the structure fosters the creation of vibrant – and valuable – developer communities, and leads to a common set of well-tested, transparent, interoperable software modules upon which the developer community can standardize.

Open source software is ubiquitous in blockchain platforms. The software code bases for Bitcoin,¹⁷ public Ethereum,¹⁸ and Hyperledger,¹⁹ and portions of the software code bases for Enterprise Ethereum²⁰ and Corda,²¹ all consist of open source software. Bitcoin and Ethereum are the leading public blockchain platforms, and Hyperledger, Corda, and Enterprise Ethereum are the “big three” leading commercial, permissioned blockchain platforms.²² Accordingly, if our hypothetical company wishes to leverage solutions that rely on software from any of these leading platforms, it must consider the impact of the licenses that govern this software.

The open source community has developed a number of licenses, and these range from (a) permissive licenses, which allow licensees royalty-free and essentially unfettered rights to use, modify, and distribute applicable software and source code,²³ to (b) restrictive, so-called “copyleft” licenses, which place significant conditions on modification and distribution of the applicable software and source code. Two open source licenses are particularly relevant to our hypothetical company: the General Public License version 3 (“GPLv3”),²⁴ because this license (and variants) governs large portions of the Ethereum code base;²⁵ and the Apache 2.0 license (the “Apache License”),²⁶ because this license governs open source software provided via the Hyperledger, Corda, and Enterprise Ethereum platforms.²⁷ Each of these licenses embodies a “reciprocity” concept that our hypothetical company must consider.

GPLv3 is known as a “strong” copyleft license. The license functions as follows: assume a developer is attracted to a software module subject to GPLv3, and incorporates this module into proprietary software that he or she then distributes to others. To the extent the developer’s proprietary software is “based on” the GPLv3 code,²⁸ the developer is required to make his or her proprietary code publicly available in source code form, at no charge,

under the terms of GPLv3. This requirement will remove trade secret protection embodied in the proprietary code, as well as the developer's ability under copyright law to control the copying, modification, distribution, and other exploitation of its software.²⁹ This license, therefore, has a significant impact on the developer's trade secret and copyright portfolios.

GPLv3 also has a significant impact on the developer's patent portfolio. The license obligates the developer to grant to all others a royalty-free license to patents necessary to make, use, or sell the Derivative Code.³⁰ Finally, simply by distributing GPLv3 code, without modification, the developer agrees to refrain from bringing a patent infringement suit against anyone else using that GPLv3 code.³¹ In sum, the structure of GPLv3 reflects a strong "reciprocal" concept: if a developer wishes to incorporate open source software into its code base, it must reciprocate by contributing that code base (and all needed IP rights) back to the community. As noted above, the Ethereum code base is licensed predominantly under GPLv3. Therefore, our hypothetical company should use caution in relying on Ethereum code.

Our hypothetical company should also consider the impact on its IP portfolio of relying on Hyperledger, Corda, and Enterprise Ethereum code. The Apache License (or an equivalent) governs large portions of these code bases. For our hypothetical company, although the Apache License has reciprocal features, it is considerably more flexible than GPLv3. The Apache License impacts a developer's rights to its software under patent, trade secret, and copyright law in a manner similar to GPLv3;³² however, these impacts only arise where the developer affirmatively contributes its software to the maintainer of the Apache code at issue. The structure functions with respect to patents as follows: if a patent owner contributes software to an Apache project, the Apache License restricts the owner from filing a patent infringement claim against any entity based on that entity's use of the contributed software. If the owner does bring such a suit, the owner's license to the Apache code underlying its contribution terminates.³³ The license thus has a reciprocal structure: a patent owner cannot benefit from Apache-licensed software while suing to enforce patents that read on its contributions to the Apache software community. If the developer, however, decides not to contribute its code to an Apache project, the developer remains free to incorporate Apache code into its proprietary code base, and commercialize this code without obligation to the Apache open source community. The Apache License, therefore, provides developers with considerable flexibility.³⁴

This flexibility may present strong value to our hypothetical company. It would permit the company, for example, to leverage existing Apache-licensed software from the Hyperledger, Corda, and Enterprise Ethereum code bases in order to develop its new platform and applications, and would give the company full control over whether and to what extent it wishes to encumber its IP portfolio with open source obligations.

Based on the above, it might appear that our hypothetical company would take extreme steps to avoid GPLv3 code (or other strong copyleft code) and would never contribute code to an Apache project. This, however, has not been the case. A number of entities have contributed code under the Apache License, for example, in order to encourage developers and users to adopt the permissioned commercial network that implements this code.³⁵ Our hypothetical company will similarly want to consider the potential benefits of seeking to create a vibrant developer and user community using an "open" approach to its IP portfolio, and potentially contributing code under an appropriate open source software license. In any event, open source software licenses and licensing techniques play a key role in blockchain technology, and our hypothetical company will want to carefully consider these licenses and techniques in its IP strategy.

The role of industry standards

Background

Industry standards refer to a set of technical specifications that a large number of industry players agree upon to use in their products.³⁶ Industry players collaboratively develop these technical specifications in a Standards Setting Organization (or “SSO”). Periodically, the SSO will hold meetings where participants, often scientists and engineers, who represent industry players will propose and debate differing proposals for how a technology should operate. Decisions regarding proposals, and the final technical specifications that stem from them, are reached by consensus of the participants.

Current efforts to standardize blockchain technology

Several organizations have begun standardizing a variety of blockchain technologies:

- The International Standards Organization (“ISO”) has formed Technical Committee 307 (“ISO/TC 307”) to consider blockchain and distributed ledger technologies.³⁷
- The Institute of Electrical and Electronics Engineers (“IEEE”) has formed two blockchain groups: (1) Project 2418 to develop a standard framework for the use of blockchain in Internet-of-Things applications;³⁸ and (2) Project 825 to develop a guide for interoperability of blockchains for energy transaction applications.³⁹
- The Blockchain in Transportation Alliance (“BiTA”) is focused on the use of blockchain in freight payments, asset history, chain of custody, smart contracts and other related goals.⁴⁰
- Hyperledger is a blockchain standard project and associated code base hosted by the Linux Foundation that focuses on finance, banking, the Internet of Things and manufacturing.⁴¹
- The Enterprise Ethereum Alliance recently released an architecture stack designed to provide the basis for an open source, standards-based specification to advance the adoption of Ethereum solutions for commercial, permissioned networks (referred to as “Enterprise Ethereum”).⁴²

Advantages and disadvantages of standards

Advantages of using and contributing to industry standards

There are several advantages to using standards that benefit an industry at large:

- **Ensures product compatibility** – With a standard in place, any vendor can develop a product that will be compatible with other products in the industry.
- **Stronger technology** – Technical specifications created with the input of many industry players tend to result in stronger overall technologies. In theory, the best ideas should emerge from the process and become industry standards that benefit both vendors and consumers.
- **Shifts competition from the standardized technology to implementation** – Standardization allows industry players to avoid competition with regard to the standardized technology, and instead shift their focus to developing the best implementation of the remaining technology. Entities that participate in the standard-setting process are obligated to disclose patents that are essential for implementing the standard, and to provide licenses to these patents on fair, reasonable, and non-discriminatory terms (so-called “FRAND” terms). These FRAND obligations ensure that all implementers will bear the same licensing burden as to patents essential to the standard.
- **Greater likelihood of wide adoption** – Approval by many industry players makes the standardized approach a “safer bet” for technology adopters and investors.

Contributing to SSOs also yields several benefits to individual participants. First, a participating company gains visibility into what comes next in their industry. For example, a software vendor for a syndicated loan blockchain platform could observe the emerging form and content of the blockchain's smart contracts and begin to steer its internal development toward efficiently processing those contracts. Second, a participating company has the opportunity to guide the standardization process. For example, steering the SSO toward smart contracts that reference cloud-based digital documents would be advantageous for a vendor with a strong cloud-based solution in place.

Disadvantages of using and contributing to industry standards

There are disadvantages to employing industry standards as well. First, a company loses control over certain aspects of the technology. Instead of developing technology in isolation, our hypothetical company can be at the whim of the industry and its own competitors. Second, a company could develop its own technology that wins over others' in the marketplace. Good faith participation in an SSO implies that a company will contribute its best, most valuable ideas to the SSO instead of applying them solely to its own products. But the prize for developing better technology than the SSO's participants, and not contributing it to the SSO, is alluring: a lucrative monopoly on the best technology. Third, an SSO is less nimble than an individual company because changes to industry standards take consensus of many parties, which in turn take time. Finally, by participating in the SSO process, the company will place FRAND obligations on any patents in its portfolio that are essential for purposes of implementing the standard.

Lessons from wireless telecommunications industry standards

Blockchain technology is a relatively new field, and SSOs are only starting to form to develop blockchain standards. Many companies are now deciding whether to join a blockchain SSO or pursue their own solutions. The history of another technical field's, e.g., telecommunications, standardization activities provides a good example of the advantages and disadvantages of pursuing industry standards or deciding to go it alone.

In order for a phone to access a carrier's wireless network, it must know how to communicate with the carrier's network. Telecommunications standards dictate how that communication proceeds. By adhering to the telecommunications standard, a manufacturer can ensure that its phone can operate on any carrier's wireless network that also follows that standard.

In the 1980s, the European "first generation" wireless telecommunications market was fractured by a handful of standards marked by national or regional boundaries. Scandinavia used a standard called "NMT;" Great Britain used "TACS;" Italy used "RTMS" and "TACS;" France used "RC2000" and "NMT;" and Germany used "C-Netz."⁴³ Using this hodgepodge of telecommunications standards meant that a German's phone would not work during her vacation to France, and an Englishman's phone would not work in Scandinavia.⁴⁴ Manufacturers for both phones and network infrastructure were likewise geographically constrained. These manufacturers would typically only research and develop products for specific European regions. What resulted were regional monopolies for those manufacturers, but with low subscriber rates and little opportunity to compete in foreign markets where their technology would be inoperable.⁴⁵

Mindful of these issues with the first generation wireless telecommunications standards, phone and infrastructure manufacturers from around Europe (and indeed around the world) came together to develop a pan-European, "second generation" standard within the European Telecommunications Standards Institute ("ETSI") SSO. These manufacturers sent their best scientists and engineers to ETSI to ensure that this emerging standard would meet wireless

subscribers' and carriers' needs. The result of their work was the Global System for Mobile communications ("GSM"), which was the *de facto* wireless standard throughout Europe and parts of the United States from 1992 through 2002. During that period, manufacturers would compete to develop better phones or network equipment, all the while maintaining compliance with the GSM standard. As a result, equipment developed in Sweden or Finland could be sold throughout Europe. This open market brought the price of wireless technology down, increased subscriber bases and, by adoption of a similar approach in the United States, ushered in today's ubiquitous smartphones and wireless networks.

Analogies can be drawn to current trends in blockchain standardization. Blockchain is based on networks that are large enough—have enough nodes—to create reliability. As such, interoperability and scalability are important. Standardization of blockchain elements can be an important tool in achieving those goals. But the standardization process often involves competing visions. Certain companies will advance one approach, and other companies will advance a different approach. That advocacy typically is based on a good faith belief, but it also arises from investments that companies make in their technology.

A meaningful standardization process contains both risk and opportunity for our hypothetical company. No company wants to make the wrong bet and become the "Betamax" or "HD DVD" of blockchain technology. Companies therefore need to be thinking hard about the competing standards that are being created and what role they wish to play in that creation. An entirely passive role can result in other thought leaders seizing the marketplace, but too aggressive a role can lead to massive investments that are not adopted by the marketplace as a whole. Ultimately, every company needs to think about the role that they wish to play on that spectrum.

* * *

Endnotes

1. There are a range of other differences between public and permissioned networks as well. For example, a permissioned network can be structured with different consensus rules that reduce the resource requirements (including electricity requirements) needed on a public network such as Bitcoin. There are also a range of gradations between fully public and fully private blockchain networks. The Enterprise Ethereum Alliance, for example, is designed to permit operation on a public network, but to restrict the nodes on that public network that receive the data at issue. See I. Allison, Enterprise Ethereum Alliance Is Back – And It's Got a Roadmap (May 2, 2018), located at <https://www.coindesk.com/enterprise-ethereum-alliance-isnt-dead-got-roadmap-prove/>.
2. Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Oct. 31, 2008) (available at <https://bitcoin.org/bitcoin.pdf>).
3. 2008 is not the earliest disclosure of blockchain-like solutions. See Stuart Haber and W. Scott Stornetta (1991) and Bayer, Haber and Stornetta (1992).
4. <https://blogs.thomsonreuters.com/answeron/in-rush-for-blockchain-patents-china-pulls-ahead>.
5. <https://blogs.thomsonreuters.com/answeron/in-rush-for-blockchain-patents-china-pulls-ahead>.
6. <https://www.lexology.com/library/detail.aspx?g=6aab712d-2ce9-401f-b37c-bffbe2aad5f>.
7. <https://finance.yahoo.com/news/chinese-tech-giants-tencent-alibaba-154422979.html>.
8. <https://finance.yahoo.com/news/chinese-tech-giants-tencent-alibaba-154422979.html>.
9. <https://finance.yahoo.com/news/chinese-tech-giants-tencent-alibaba-154422979.html>.

10. <https://harrityllp.com/top-companies-in-blockchain-patents/>.
11. <https://www.ibm.com/blockchain>.
12. <https://www.delltechnologies.com/en-us/perspectives/tags/blockchain>.
13. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).
14. Certain industry participants have been working to place restrictions on key patents, to prevent them from being acquired by NPEs. See Michael del Castilloite, Patent Trolls Beware: 40 Firms Join Fight Against Blockchain IP Abuse (March 16, 2017) located at <https://www.coindesk.com/40-blockchain-firms-unite-in-fight-against-patent-trolls/>.
15. 35 U.S. Code § 154(a)(1) (“Every patent shall . . . grant to the patentee, his heirs or assigns, of the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States . . .”).
16. <https://blog.coinbase.com/how-we-think-about-patents-at-coinbase-26d82b68e7db>.
17. See <http://www.Bitcoin.org>.
18. L. Zeug, “Licensing” (September 4, 2016), located at <https://github.com/ethereum/wiki/wiki/Licensing>.
19. “About Hyperledger,” located at <https://www.hyperledger.org/about>.
20. Enterprise Ethereum Alliance Specification Clears the Path to a Global Blockchain Ecosystem (May 16, 2018), located at <https://entethalliance.org/enterprise-ethereum-alliance-specification-clears-path-global-blockchain-ecosystem/>.
21. “Contributing to Corda,” located at <https://github.com/corda/corda/blob/master/CONTRIBUTING.md>; Downloads: DemoBench for Corda 3.0, located at <https://www.corda.net/downloads/>.
22. R. Brown, “Corda: Open Source Community Update” (May 13, 2018) located at <https://medium.com/corda/corda-open-source-community-update-f332386b4038>.
23. Bitcoin software, for example, is licensed under the permissive, MIT License. See <http://www.Bitcoin.org>; <https://opensource.org/licenses/MIT>.
24. GPLv3 license, located at <https://www.gnu.org/licenses/gpl-3.0.en.html>.
25. L. Zeug, “Licensing” (September 4, 2016), located at <https://github.com/ethereum/wiki/wiki/Licensing>. See, e.g., Ethereum-sandbox License, located at <https://github.com/ether-camp/ethereum-sandbox/blob/master/LICENSE.txt>.
26. Apache 2.0 license, located at <https://www.apache.org/licenses/LICENSE-2.0>.
27. For Corda, see R. Brown, “Corda: Open Source Community Update” (May 13, 2018) located at <https://medium.com/corda/corda-open-source-community-update-f332386b4038>; “Contributing to Corda,” located at <https://github.com/corda/corda/blob/master/CONTRIBUTING.md>. For Hyperledger, see Brian Behlendorf, “Meet Hyperledger: An ‘Umbrella’ for Open Source Blockchain & Smart Contract Technologies” (September 13, 2016) located at <https://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies>. Code contributed to the Enterprise Ethereum Alliance is generally made available under an open source license that mirrors the Apache 2.0 license, see Enterprise Ethereum Alliance Inc. Intellectual Property Rights Policy, available at <https://entethalliance.org/join/>.
28. In defining the key term “based on,” GPLv3 largely relies on copyright law rules governing derivative works. Courts generally rule that two copyrighted works are distinct (and one is not derivative of the other) if “they can live their own copyright life;” in other words, the test focuses on whether each expression “has an independent economic value and is, in itself, viable.” E.g., *Columbia Pictures Indus. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1192 (9th Cir. 2001); *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, 964 F.2d 965, 969 (9th Cir. 1992).
29. For convenience, the code the developer is required to open-source in this manner is referred to as “Derivative Code.”

30. GPLv3, sec. 11 (Patents).
31. GPLv3, sec. 10 (Automatic Licensing of Downstream Recipients).
32. The maintainer of the relevant Apache code at issue, through the Apache Software Foundation, has the ability to set downstream terms for the contributed software.
33. Apache 2.0, sec. 3 (Grant of Patent License).
34. Our hypothetical company will also need to consider “compatibility” issues between various open source licenses. The Hyperledger platform, for example, was unable to assimilate Ethereum code due to incompatibility between the Apache License and strong copyleft licenses, and the resulting need to obtain permissions from copyright owners to “re-license” the Ethereum code at issue. See J. Manning, *Hyperledger Fails Ethereum Integration Due To Licensing Conflicts* (February 3, 2017), located at <https://www.ethnews.com/hyperledger-fails-ethereum-integration-due-to-licensing-conflicts>; J. Buntinx, *Ethereum app Developers may Face Licensing Issues Later on* (December 6, 2017), located at <https://www.newsbtc.com/2017/12/06/ethereum-app-developers-may-face-licensing-issues-later/>.
35. IBM, for example, has contributed code under the Apache License to the Hyperledger platform, and in turn is providing commercial Blockchain-as-a-Service (“BaaS”) offerings based on this platform using IBM’s cloud infrastructure. See IBM Blockchain, *The Founder’s Handbook: Your guide to getting started with Blockchain* (Edition 2.0) located at <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=28014128USEN>. Microsoft has similar commercial offerings, based on Azure and the Enterprise Ethereum platform. See M. Finley, *Getting Started with Ethereum using Azure Blockchain* (January 24, 2018), located at https://blogs.msdn.microsoft.com/premier_developer/2018/01/24/getting-started-with-ethereum-using-azure-blockchain/.
36. A simple example is the shape and voltage of a wall power outlet. Because the power outlet is standardized among geographic regions, an appliance-maker can ensure that its coffee-maker will work (and can be sold) anywhere within a given region.
37. <https://www.iso.org/committee/6266604.html>.
38. <http://standards.ieee.org/develop/project/2418.html>.
39. <http://standards.ieee.org/develop/project/825.html>.
40. <https://bita.studio>.
41. <https://www.hyperledger.org>.
42. Enterprise Ethereum Alliance Advances Web 3.0 Era with Public Release of the Enterprise Ethereum Architecture Stack (May 2, 2018), located at <https://entethalliance.org/enterprise-ethereum-alliance-advances-web-3-0-era-public-release-enterprise-ethereum-architecture-stack/>; <https://entethalliance.org/wp-content/uploads/2018/05/EEA-TS-0001-0-v1.00-EEA-Enterprise-Ethereum-Specification-R1.pdf>.
43. Funk, Jeffrey L., *Global Competition Between and Within Standards: The Case of Mobile Phones* at 39 (New York, Palgrave, 2002); Garrard, Garry A., *Cellular Communications: Worldwide Market Development* (Boston, Artech House, 1998).
44. Gruber, Harald, *The Economics of Mobile Telecommunications* at 35 (Cambridge University Press, 2005).
45. *Id.*

* * *

Acknowledgment

The authors would like to thank Jacob Schneider for his valuable contribution to this chapter.

**Joshua Krumholz****Tel: +1 617 573 5820 / Email: joshua.krumholz@hkllaw.com**

Josh Krumholz is a partner in Holland & Knight's Boston office. A trial attorney and the national Practice Group Co-Leader for the firm's Intellectual Property Group, Mr Krumholz focuses primarily upon intellectual property litigation, with a particular focus on patent litigation. His practice covers a variety of technologies and jurisdictions. Mr Krumholz has successfully taken cases to jury verdict in the Eastern District of Texas, Illinois, Massachusetts, New Jersey and New York, among other jurisdictions. Technologies that Mr Krumholz handles include telecommunications, software, hardware, electronics and consumer goods. Mr Krumholz represents leading companies across a range of industries, including Ericsson Inc., T-Mobile, Inc., Verizon Corp., Avaya Inc., Acushnet Company and Hasbro, Inc., among others.

**Ieuan G. Mahony****Tel: +1 617 573 5835 / Email: ieuan.mahony@hkllaw.com**

Ieuan Mahony is a partner in Holland & Knight's Boston office. He concentrates his practice in intellectual property (IP) licensing and development, data privacy and security, and information technology (IT). Mr Mahony combines his transactional and compliance work with dispute resolution and litigation matters. His substantial background in transactional and litigation practice areas helps clients receive high-quality advice in the dynamics of reaching an agreement as well as the realities of combating an adversary. Mr Mahony is a member of the firm's three-partner Information Technology Governance Committee.

**Brian J. Colandreo****Tel: +1 617 305 2143 / Email: brian.colandreo@hkllaw.com**

Brian Colandreo is a partner in Holland & Knight's Boston office. Mr Colandreo serves as the National Patent Practice Leader and is a member of the Intellectual Property Group. A registered patent attorney, Mr Colandreo focuses his practice on client management, general intellectual property prosecution, transactional work, litigation support, due diligence work, and utility and design patent opinion work. Prior to entering law school, Mr Colandreo worked as a systems/software engineer for Johnson Controls.

Holland & Knight LLP

800 17th Street N.W., Suite 1100, Washington, D.C. 20006, USA
Tel: +1 202 955 3000 / Fax: +1 202 955 5564 / URL: www.hkllaw.com

Cryptocurrency and other digital asset funds for U.S. investors

Gregory S. Rowland & Trevor I. Kiviat
Davis Polk & Wardwell LLP

Introduction

In 2008, an unknown author publishing under the name Satoshi Nakamoto released a white paper describing Bitcoin, a peer-to-peer version of electronic cash, and the corresponding software that facilitates online payments directly between counterparties without the need for a financial intermediary. In the decade that has followed, Bitcoin and countless other open-source, decentralised protocols inspired by Bitcoin (for example, Ethereum and Monero) have come to represent a \$300 billion-plus market of alternative assets, commonly referred to as “digital assets”, which are typically traded over the internet using online exchange platforms.

Digital assets can serve several functions. Although the following categories are not independent legal categories under U.S. law, such distinctions are helpful for understanding and crafting various investment strategies involving these assets. Some digital assets, such as Bitcoin or Litecoin, are widely regarded as decentralised stores of value or mediums of exchange due to certain common economic features that support these functions; these are sometimes referred to as “pure cryptocurrencies”. Other digital assets, such as Monero or Zcash, are a subset of pure cryptocurrencies that also possess certain features designed to enhance transaction privacy and confidentiality (“privacy-focused coins”).

Beyond pure cryptocurrencies and privacy-focused coins, there exists a broad array of general purpose digital assets (“platform coins”), such as Ethereum, NEO and Ravencoin, which are designed to facilitate various peer-to-peer activities, from decentralised software applications to “smart” contracts to digital collectibles, such as CryptoKitties. Platform coins also enable the creation of new digital assets called “tokens”, which are typically developed for a specific purpose or application – for example, (1) “utility tokens”, which generally are designed to have some consumptive utility within a broader platform or service, or (2) “security tokens”. The latter are designed to represent more traditional interests like equity, debt and real estate with the added benefit of certain features of the digital asset markets, such as increased liquidity, more cost-effective fractional interest transfers, more efficient cross-border trading, faster and more transparent payment of dividends and other distributions and rapid settlement.

The digital asset market extends beyond the assets themselves. Other participants, including online exchanges, payment processors and mining companies, compose the broader digital asset industry. And as this industry continues to grow, it has captured the attention of retail and institutional investors alike, including asset managers seeking to develop investment strategies and products involving these emerging assets and companies. Some strategies resemble early-stage growth strategies, featuring long-term investments either directly in certain digital assets

or in start-up ventures developing complementary goods and services for the industry. Other strategies include hedge fund strategies, such as long/short funds, which often use derivatives, or arbitrage strategies, which seek to capitalise on the price fragmentation across the hundreds of global online exchanges. Additionally, during periods of weak or middling performance in the cryptocurrency markets – for example, during the so-called “crypto winter” of 2018–19¹ – fund managers began experimenting with novel revenue-generation strategies, such as staking cryptocurrencies,² adopting credit fund-type strategies (e.g., distressed debt), engaging in market-making and executing venture capital investments.

This chapter outlines the current U.S. regulatory and tax framework applicable to cryptocurrency and other digital asset investment funds (“digital asset funds”) offered to U.S. investors and how those regulatory and tax considerations affect fund-structuring decisions.

The U.S. regulatory framework generally

Digital asset funds operated in the United States or offered to U.S. investors must contend and comply with a complex array of statutes and regulations. These include: the Securities Act of 1933 (the “Securities Act”), which regulates the offer and sale of securities; the Investment Company Act of 1940 (the “1940 Act”), which regulates pooled investment vehicles that invest in securities; the Commodity Exchange Act (the “CEA”), which regulates funds and advisers that trade in futures contracts, options on futures contracts, commodity options and swaps; and the Investment Advisers Act of 1940 (the “Advisers Act”), which governs investment advisers to such funds. Additionally, many fund-structuring decisions are driven by tax considerations. This section sets out the current U.S. regulatory framework applicable to digital asset funds managed in the United States or offered to U.S. investors and explores how those regulatory considerations affect fund-structuring decisions.

Offering of fund interests

Interests in investment funds are securities. Under the Securities Act, an offering of securities must be registered with the U.S. Securities and Exchange Commission (“SEC”) or made pursuant to an exemption. While there are a few possible exemptions, the most common exemption that private funds rely upon is Regulation D, which provides two alternative exemptions from registration: Rule 504 and Rule 506. Because most private investment funds intend to raise more than \$5 million, Rule 506, which provides no limit on the amount of securities that may be sold or offered, is the exemption under Regulation D most commonly relied on by such funds, and consequently, this discussion of Regulation D is limited to offerings made under Rule 506.³ In order to offer or sell securities in reliance on Rule 506 of Regulation D, an investment fund must:

- limit sales of its securities to no more than 35 non-accredited investors (unless the offering is made pursuant to Rule 506(c), in which case all purchasers must be accredited investors), although securities may be sold to an unlimited number of accredited investors;
- ensure that all non-accredited investors meet a sophistication requirement by having such knowledge and experience in financial and business matters that they are capable of evaluating the merits and risks of the prospective investment;
- refrain from general solicitation or advertising in offering or selling securities (unless the offering is made pursuant to Rule 506(c));
- comply with the information disclosure requirements of Rule 502(b) with respect to any offering to non-accredited investors. There are no specific information requirements for offerings to accredited investors;

- implement offering restrictions to prevent resales of any securities sold in reliance on Regulation D; and
- file a Form D notice of the offering with the SEC within 15 calendar days of the first sale of securities pursuant to Regulation D.

There are also some important limitations on the scope of the Regulation D exemption. For example, Regulation D only exempts the initial transaction itself (i.e., resales of securities acquired in an offering made pursuant to Regulation D must be either registered or resold pursuant to another exemption from registration). Furthermore, Regulation D is not available for any transaction or series of transactions that, while in technical compliance with Regulation D, is deemed to be part of “a plan or scheme to evade the registration provisions of the [Securities] Act”.

The regulatory treatment of cryptocurrencies and other digital assets

As discussed above, interests in investment funds themselves are securities; however, these funds may hold a variety of different assets in pursuing their respective strategies – from digital assets (e.g., Bitcoin and Ether) to derivatives instruments (e.g., Bitcoin futures contracts) to securities (e.g., equity in an emerging growth company or interests in another digital asset fund). This section provides an overview of the regulatory treatment of such assets, particularly with respect to the definitions of “securities” under the U.S. securities laws and “commodity interests” under the CEA, before explaining how these characterisations impact structuring decisions. Although some generalisations may be inferred about the possible treatment of certain assets based on common features and fact patterns, there is no substitute for a careful case-by-case analysis of each asset, in close consultation with counsel.

In July 2017, in a release commonly referred to as the DAO Report,⁴ the SEC determined that certain digital assets are securities for purposes of the U.S. federal securities laws. The DAO Report was published in response to a 2016 incident in which promoters of an unincorporated virtual organisation (“The DAO”) commenced an initial coin offering (an “ICO”), a term that generally refers to a sale of tokens to investors in order to fund the development of the platform or network in which such tokens will be used. The DAO was created by a German company called Slock.it, and it was designed to allow holders of DAO tokens to vote on projects that The DAO would fund, with any profits flowing to token-holders. Slock.it marketed The DAO as the first instance of a decentralised autonomous organisation, powered by smart contracts on a blockchain platform. The DAO’s ICO raised approximately \$150 million (USD) in Ether.

In the DAO Report, the SEC reasoned that the DAO tokens were unregistered securities because they were investment contracts, which is one type of security under the U.S. securities laws. Though it declined to take enforcement action against The DAO, the SEC used this opportunity to warn others engaged in similar ICO activities that an unregistered sale of digital assets can, depending on the facts and circumstances, be an illegal public offering of securities. The SEC has relied on similar reasoning in subsequent actions taken against token issuers that deem certain other digital assets sold in ICOs to be securities (such securities, “DAO-style tokens”).⁵ Many DAO-style tokens are branded by their promoters as utility tokens to convey the idea that such tokens are designed to have some consumptive utility within a broader platform or service. But as noted above, this terminology does not have any legal consequence under the U.S. securities laws. Instead, a proper inquiry must examine the facts and circumstances surrounding the asset’s offering and sale, including the economic realities of the transaction.⁶ Key factors to consider include: (1) whether a

third party – be it a person, entity or coordinated group of actors – drives the expectation of a return; and (2) whether the digital asset, through contractual or other technical means, functions more like a consumer item and less like a security.⁷ Additionally, in April 2019, the SEC staff published new detailed guidance on when a digital asset may be considered a security, in the form of two documents: a framework issued by the SEC’s Strategic Hub for Innovation and Financial Technology along with a no-action letter from the SEC’s Division of Corporation Finance. The framework reaffirms the staff’s position that digital assets sold to investors to raise capital are generally securities, regardless of potential utility, and charts a narrow path for the sorts of digital assets that the staff would not consider a security. Meanwhile, the no-action relief is narrow and unlikely to provide meaningful guidance or practical utility for many types of currently available digital assets or firms considering issuing digital assets.⁸ Finally, while it is beyond the scope of this chapter, the SEC has taken numerous enforcement actions against ICO issuers in cases where it believes that the offer and sale of the particular tokens in question amounted to an unregistered offering of securities.⁹

In addition to DAO-style tokens, some digital assets are explicitly designed to be treated as securities from the outset and are meant to represent traditional interests like equity and debt, with the added benefit of certain features of the digital asset markets, such as 24/7 operations, fractional ownership and rapid settlement. These digital assets are securities by definition, and although they represent an innovation in terms of how securities trade, clear and settle, they are not necessarily a new asset class.

Any cryptocurrencies or other digital assets that are not deemed to be securities under the U.S. securities laws may be considered “commodities” under the CEA, due to the broad definition of the term.¹⁰ For example, the U.S. Commodity Futures Trading Commission (“CFTC”) appears to be treating Bitcoin as an exempt commodity under the CEA, a category that includes metals and energy products,¹¹ but does not include currencies or securities, which are classified as excluded commodities.¹² Additionally, in December 2017, the CFTC permitted the self-certification of futures contracts and binary options on Bitcoin by futures exchanges under its rules for listing ordinary futures contracts.¹³ And although the SEC has not taken any action with respect to Bitcoin specifically, SEC Chairman Jay Clayton has acknowledged, and appeared to accept as correct, the CFTC’s designation of Bitcoin as a commodity over which the CFTC has anti-fraud jurisdiction.¹⁴ Finally, to the extent that a digital asset is a commodity, any derivatives offered on that commodity – for example, Bitcoin futures contracts and binary options – fall squarely within the definition of commodity interests under the CEA.

Possible obligations of the manager under the Advisers Act or the CEA

The question of whether a digital asset fund manager must comply with additional regulations under either, or both, the Advisers Act and the CEA turns primarily on the characterisation of the assets its funds hold. First, a manager is deemed an “investment adviser” under Section 202(a)(11) of the Advisers Act, and thus is subject to the rules and regulations thereunder, if it “for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities”, or “for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities”. So to the extent that a manager of a cryptocurrency or other digital asset fund is advising on “securities” – for example, because its funds hold DAO-style tokens or security tokens – it must register as an investment advisor with the SEC unless such individual or entity qualifies for an exclusion from the definition or an exemption from the registration requirement.¹⁵

Registration under the Advisers Act subjects advisers to a host of rules and regulations, including those governing advertising, custody, proxy voting, record-keeping, the content of advisory contracts, and fees. For example, the Advisers Act custody rule¹⁶ (the “custody rule”) has detailed provisions applicable to any SEC-registered investment adviser deemed to have custody, as defined under the rule. Among other things, it requires use of a “qualified custodian” to hold client funds or securities, notices to clients detailing how their assets are being held, account statements for clients detailing their holdings, annual surprise examinations and additional protections when a related qualified custodian is used. For example, investment advisers dealing in digital assets may need to consider whether a bank, registered broker-dealer, or other firm that meets the definition of a qualified custodian, is willing to take custody of the digital assets.

Second, managers of private funds that invest or trade in “commodity interests”, whether as an integral part of their investment strategy or only in a limited capacity, for hedging purposes or otherwise, are subject to regulation under the CEA and the rules of the CFTC thereunder (“CFTC Rules”). Commodity interests generally include: (1) futures contracts and options on futures contracts; (2) swaps; (3) certain retail foreign currency and commodity transactions; and (4) commodity options and certain leveraged transactions. So to the extent that the activities of a manager of a cryptocurrency or other digital asset fund include trading in commodity interests – for example, because it holds Bitcoin futures contracts or binary options – it will be subject to registration and regulation as a commodity pool operator (“CPO”) or commodity trading advisor (“CTA”), unless it qualifies for an exemption or exclusion under the CEA or the CFTC Rules.

If the activities of an investment fund bring it within the definition of a “commodity pool” under the CEA, the manager is required to register as a CPO with the CFTC, unless such person otherwise qualifies for an exclusion from the definition of CPO or an exemption from the registration requirement. The CEA also provides for the registration of CTAs, which is in some respects analogous to the treatment of investment advisers under the Advisers Act. It should be noted, however, that numerous requirements under the CEA and the CFTC Rules apply to all CPOs and CTAs, even those that are exempt from registration.

Possible obligations of the fund under the 1940 Act or the CEA

Similarly, the fund itself may be subject to additional regulations under either, or both, the 1940 Act and the CEA, an analysis that, again, turns primarily on the assets the fund holds. An investment company is defined under Section 3(a)(1)(A) of the 1940 Act as any issuer that “is or holds itself out as being engaged primarily, or proposes to engage primarily, in the business of investing, reinvesting or trading in securities”. This subjective test is based generally on how a company holds itself out to the public and the manner in which it pursues its business goals, and is designed to capture traditional investment companies that are deliberately acting in that capacity. Additionally, Section 3(a)(1)(C) of the 1940 Act sets forth an objective, numerical test that applies to companies that hold a significant portion of their assets in investment securities, even if they do not hold themselves out as traditional investment companies.

Companies that fall within one of these definitions of an investment company must either satisfy an exemption from the 1940 Act or register under it. The 1940 Act is a comprehensive statutory regime that imposes strict requirements on registered investment companies’ governance, leverage, capital structure and operations. Consequently, most private equity funds, hedge funds and other alternative investment vehicles, which fall squarely within the definition of “investment company”, are structured to satisfy an exemption from the 1940 Act.

The 1940 Act provides specific exemptions from the definition of “investment company” for privately offered investment funds and certain other types of companies. For example, Section 3(c)(1) exempts a private investment fund from registration if the outstanding securities of such fund (other than short-term paper) are beneficially owned by not more than 100 persons and such fund does not presently propose to make a public offering of its securities. Further, Section 3(c)(7) excludes an entity from registration as an investment company if all of the beneficial owners of its outstanding securities are “qualified purchasers” and the entity does not make or propose to make a public offering of its securities, and it does not limit the number of beneficial owners.

The CEA defines “commodity pool” as any investment trust, syndicate or similar form of enterprise operated for the purpose of trading in commodity interests. The CFTC interprets “for the purpose” broadly and has rejected suggestions that trading commodity interests must be a vehicle’s principal or primary purpose. As a result, any trading by a private fund in swaps, futures contracts or other commodity interests, no matter how limited in scope, and regardless of whether undertaken for hedging or speculative purposes, generally will bring a private fund within the commodity pool definition.

According to the CFTC, a fund that does not trade commodity interests directly but invests in another fund that trades commodity interests would itself be a commodity pool. Thus, in a master-feeder fund structure, a feeder fund will be considered a commodity pool if the master fund is a commodity pool. Similarly, a fund of funds that invests in commodity pools may itself be considered a commodity pool.

Finally, an investment vehicle can be both an “investment company” under the 1940 Act and a “commodity pool” under the CEA, and an exception from the registration requirements of the 1940 Act does not generally imply an exception from CPO registration under the CEA (or *vice versa*). Similarly, an exception from registration under the Advisers Act does not generally imply an exception from CTA registration (or *vice versa*). Furthermore, interests in commodity pools are “securities” under the Securities Act, and therefore the Securities Act applies to the offer and sale of interests in a commodity pool to the same extent as it applies to any other type of security. Accordingly, offering of interests in a private fund that is a commodity pool generally will be structured to meet the requirements of a Securities Act exemption (e.g., Regulation D, as discussed above).

Applying this framework to digital asset funds

Given the regulatory minefield laid out above, managers face a multitude of structuring decisions in conceiving and launching digital asset funds aimed at U.S. investors. These decisions will often influence, and be influenced by, the manager’s investment strategy – particularly as it relates to the types of assets the fund should be permitted to hold. This section explores some common structures and the strategies they support. In each of these cases, one should keep in mind that interests in the digital asset fund itself are securities, as noted above, that must be offered and sold pursuant to an exemption, such as Regulation D, except in the case of registered (i.e., public) funds, which are offered and sold in fully registered securities offerings.

First, the manager may decide that the fund should have flexibility to invest in securities. It may want to invest in “traditional” securities like equity or debt in a company within the digital asset industry (including through tokenised securities), or DAO-style tokens and other digital assets at risk of being deemed investment contracts. In this case, the adviser will likely need to register under the Advisers Act and comply with the host of rules and regulations thereunder, including those governing advertising, custody, proxy voting,

record-keeping, the content of advisory contracts, and fees. Non-U.S. advisers, however, can potentially rely on Advisers Act Rule 203(m)-1 (the “private fund adviser rule”).¹⁷

Custody poses unique questions in the digital asset context, and it is not clear in all cases whether digital assets would be viewed as funds or securities, such that the custody rule would apply. Currently, most qualified custodians do not offer custody services for digital assets. In any case, the manager should familiarise itself with the operational considerations of digital asset custody. First, what does it mean to have custody of an asset that is not physical and, even in digital form, does not exist on a centralised database, but instead on one that is universal and distributed? For example, one cannot physically move units of Bitcoin off of the Bitcoin blockchain and store them elsewhere. However, in order to exercise control over one’s Bitcoins, one needs a private and a public key. These keys are a series of hexadecimal characters (e.g., 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa), which must be stored carefully. The public key is the identity of the address on the network that has ownership and control of those Bitcoins – this key can be shared with anyone, and in fact, it must be shared in order to receive Bitcoins. The private key is essentially a password, and Bitcoins can be transferred out of a particular address by anyone with possession of that address’s corresponding private key. So, in the case of a blockchain-based asset like Bitcoin, control of the private key may be tantamount to custody. As there is simply no recourse to retrieve Bitcoins when a private key is lost or stolen, a critical operational point for managers is safe and secure private key storage; for example, through “deep cold” storage.¹⁸

If the manager believes the digital asset fund may invest in securities, the fund itself would likely be structured so as to meet one of the various registration exemptions for entities that would otherwise be classified as “investment companies” under the 1940 Act.¹⁹ For offshore funds, the requirements of Sections 3(c)(1) and 3(c)(7), which are discussed above, generally only apply to U.S. investors.

Alternatively, the manager may consider structuring the fund as a registered investment company, although as of the date of this chapter, the SEC has not approved any such funds. As the authors discuss in “The Current State of U.S. Public Cryptocurrency Funds”, there have been a number of requests to list on national securities exchanges the shares of such funds.²⁰ The SEC has repeatedly denied such requests, and in January 2018, the SEC’s Division of Investment Management outlined several questions that sponsors would be expected to address before it would consider granting approval for funds holding “substantial amounts” of cryptocurrencies or “cryptocurrency-related products”.²¹ The questions, which focus on specific requirements of the 1940 Act, generally fall into one of five key areas: valuation; liquidity; custody; arbitrage; and potential manipulation. And although such funds alternatively could potentially be offered to the public as non-investment companies (to the extent they do not hold significant amounts of securities) under the Securities Act, the SEC has indicated that significant, similar questions exist there also.²²

Second, the manager may decide that the fund should have flexibility to invest in commodity interests, such as futures contracts or binary options, either for hedging or speculative purposes. Any such trading by a private fund, no matter how limited in scope, and regardless of the purpose, would generally make such fund a “commodity pool”, as discussed above. In this case, the manager may be required to register as a CPO or CTA with the CFTC, although certain exemptions exist for non-U.S. managers and for funds that invest in only limited amounts of commodity interests. Even if the manager decides that such fund should only invest in commodity interests and not securities, interests in commodity pools are “securities” under the Securities Act, and therefore, the fund would generally be structured to meet the requirements of a Securities Act exemption (e.g., Regulation D, as discussed above).

Finally, the manager may decide that the fund should hold neither securities nor commodity interests – in other words, a fund that holds only commodities, or “pure cryptocurrencies”, such as Bitcoin, and no commodity interests. Because this category does not have independent legal significance under U.S. law, such determinations regarding the risk that a given digital asset could be deemed a “security” for U.S. securities laws purposes should be made carefully and together with legal counsel. In this case, the fund would not be governed by the 1940 Act, and the manager’s activities with respect to the fund would not be governed by the Advisers Act, as both of these regimes are premised upon the fund holding securities, as discussed above. Further, because the fund does not hold commodity interests, it would likely not be considered a “commodity pool”, and the manager would likely not be required to register as a CPO or CTA with the CFTC. However, the fund and the manager in this case would not be entirely unregulated. As noted above, interests in the fund are securities (regardless of the underlying assets that the fund invests in), the offer and sale of which must comply with U.S. securities laws. Additionally, the CFTC has some, albeit limited, jurisdiction over the spot market for commodities pursuant to its anti-fraud and manipulation authority.²³ Moreover, the manager of such a fund would likely be considered a common law fiduciary to such a fund and thus subject to fiduciary duties in its management of the fund.

U.S. federal income tax framework

Tax considerations are often a principal driver for managers when deciding how to structure an investment fund. For managers of funds that invest in or trade digital assets, these structuring decisions are particularly complex given the limited guidance and uncertainty that exist with respect to the treatment of digital assets for U.S. federal income tax purposes.

The U.S. federal income tax treatment of cryptocurrencies and other digital assets

Through three pieces of published guidance, the U.S. Internal Revenue Service (“IRS”) has established a limited framework for analysing the U.S. federal income tax consequences of digital asset transactions. In Notice 2014-21 (the “Notice”),²⁴ the IRS established that “virtual currency”, defined as a “digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value”, is treated as “property” that is not “currency” and, therefore, that general tax principles applicable to property transactions apply to transactions using virtual currency. Thus, for example, assuming that a taxpayer holds a unit of virtual currency as a capital asset (which includes property held for investment purposes), a disposition of that virtual currency will result in capital gain or loss to the taxpayer. In 2019, the IRS simultaneously released a revenue ruling²⁵ and a series of “frequently asked questions”²⁶ (the “Ruling & FAQs”) that provide additional guidance with respect to the taxation of virtual currency. The Ruling & FAQs establish the IRS’s position that a hard fork of virtual currency will give rise to taxable ordinary income equal to the fair market value of the new virtual currency that arises as a result of the fork if a taxpayer is able to exercise “dominion and control” over that new virtual currency,²⁷ and provide guidance on a number of other ancillary issues relevant to the taxation of virtual currency (including matters relating to basis, holding period and certain other tax accounting issues).

Despite this guidance, there are many aspects of the taxation of digital assets that remain unclear, including issues that are of particular import to fund managers when considering how to efficiently structure a fund that invests in or trades digital assets. These areas of uncertainty include whether: (i) income and gain from digital assets constitutes, for instance, “qualifying income” for purposes of the publicly traded partnership rules, or “passive income” for purposes of the “passive foreign investment company” (or “PFIC”) rules;

(ii) income from forks, airdrops or similar occurrences (“fork-type income”) constitutes “unrelated business taxable income” (or “UBTI”) for U.S. tax-exempt investors; (iii) fork-type income is subject to non-resident alien tax withholding;²⁸ and (iv) whether a loan of digital assets is a taxable event.²⁹

Applying this framework to digital asset funds

Many private investment fund structures consist of at least two vehicles: a vehicle that is treated as a partnership for U.S. federal income tax purposes (a “Master Fund”); and a vehicle that is organised in a non-U.S. jurisdiction³⁰ and is treated as a corporation for U.S. federal income tax purposes (an “Offshore Fund”). U.S. taxable investors generally invest (directly or through other partnership fund vehicles) in the Master Fund, and, because partnerships receive “pass-through” treatment for U.S. tax purposes, the U.S. investors generally are treated as if they directly derived their shares of the Master Fund’s items of taxable income, gains, losses and deductions. Non-U.S. and U.S. tax-exempt investors generally invest in the Offshore Fund in order to “block” certain types of income that could cause adverse tax consequences to those investors if received directly. Other investment fund structures utilise a single partnership or corporate vehicle. The choice of fund structure for a digital asset investment vehicle may be informed by the manager’s investment strategy and the composition of the vehicle’s investor base.

As noted above, many private investment funds include a Master Fund designed to be treated as a partnership for tax purposes. In that regard, the “publicly traded partnership” rules of the U.S. Internal Revenue Code of 1986, as amended (the “Code”), provide that if interests in a partnership are traded on an established securities market or are readily tradable on a secondary market, the partnership generally will be treated as a corporation for U.S. federal income tax purposes, unless at least 90% of the partnership’s income for each taxable year consists of “qualifying income”.³¹ While there are strong arguments, both based on the statutory text of Section 7704 of the Code (as well as the relevant Treasury Regulations) and from a tax policy perspective, for treating income and gains from investments in digital assets as “qualifying income”, the lack of guidance on this issue has left fund managers facing a trade-off between the tax efficiency of a pass-through vehicle and liquidity for investors. To ensure that the Master Fund does not become subject to corporate-level U.S. tax, managers often restrict the number of persons that may invest in the fund or the frequency with which investors are able to transfer or redeem their interests.

Where a partnership is used as a digital asset investment vehicle (even where the activities of the fund do not constitute the conduct of a trade or business in the United States, such that a non-U.S. investor could conceivably invest directly in the fund), the use of an offshore “blocker” corporation might be necessary to attract tax-exempt investors. In particular, uncertainty regarding whether fork-type income constitutes UBTI could cause U.S. tax-exempt investors to favour holding any investments in digital assets through a “blocker” corporation.³²

In addition to using non-U.S. corporations as “blockers”, managers that seek to offer greater liquidity in their digital asset funds than might be available through a partnership structure (because of the reasons described above) sometimes offer interests in a non-U.S. corporate investment vehicle to taxable U.S. investors. However, the consequences to a taxable U.S. investor of investing in such vehicles are also subject to some uncertainty. In particular, the IRS’s position in the Ruling & FAQs that a hard fork of virtual currency can give rise to taxable income calls into question whether such funds will be treated as PFICs.³³ Classification as a PFIC can result in significant administrative and reporting burdens for

the corporation and its shareholders and, absent certain elections, U.S. shareholders in a PFIC are generally subject to disadvantageous tax consequences.

The preceding discussion addresses but a few of the myriad structuring and other tax considerations implicated by investments in digital assets, others of which are similarly subject to uncertainty given the nascent state of guidance in the area. As the tax law applicable to investments in digital assets continues to develop, managers and their advisors must carefully consider and plan for these issues.

Conclusion

Over the past decade, digital assets have come a long way – from Satoshi’s original Bitcoin white paper to today’s broad universe of 5,000-plus digital assets trading across hundreds of online trading platforms. As this market and the surrounding industry matures, asset managers will likely continue to identify opportunities to either deploy novel investment strategies or adapt their tried-and-true strategies in this new context. As set out above, such managers face a complex array of statutes and regulations in offering digital asset funds to U.S. investors and optimising their funds’ tax characteristics. These considerations, together with the investment strategies that the manager desires to pursue, affect fund-structuring decisions, and accordingly, are best addressed together with counsel.

* * *

Endnotes

1. Proof of Stake – Bitcoin Wiki, https://en.bitcoin.it/wiki/Proof_of_Stake (last visited Aug. 3, 2020) (staking involves users locking tokens in a wallet that is then used to secure the network, validate transactions and produce new blocks, thereby allowing users to earn a passive income return). These additional activities, such as market-making, may raise additional U.S. regulatory issues that are beyond the scope of this chapter.
2. Frank Chaparro, Crypto hedge funds are getting creative as the bear market tightens its grip, *The Block* (2018), <https://www.theblockcrypto.com/2018/12/04/crypto-hedge-funds-are-getting-creative-as-the-bear-market-continues-to-grip-crypto/> (last visited Aug. 3, 2020).
3. Historically, issuers and any persons acting on their behalf were prohibited from engaging in any form of general solicitation or general advertising in Rule 506 offerings. However, in July 2013, the SEC adopted final rules to permit general solicitation and general advertising in Rule 506 offerings under new Rule 506(c). Additional requirements apply to Rule 506(c) offerings, including the requirement to take reasonable steps to verify an investor’s accredited investor status. Under Rule 506(b), an investment fund may offer securities pursuant to Rule 506 without complying with these additional requirements if it does not use general solicitation. Currently, most private funds offered in the United States choose not to use general solicitation.
4. SEC Release No. 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Jul. 25, 2017).
5. *See, e.g.*, SEC Release No. 10445, *In the matter of Munchee, Inc.* (Dec. 11, 2017).
6. This includes, for example, (1) whether the investor’s fortunes are interwoven with those of other investors or the efforts of the promoter of the investment, and (2) whether the investor’s expectation of profits are based predominantly upon the entrepreneurial or managerial efforts of the promoter or other third parties. *See SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

7. Director William Hinman, Remarks at the Yahoo Finance All Markets Summit, *Asset Transactions: When Howey Met Gary (Plastic)* (Jun. 14, 2018), available at <https://www.sec.gov/news/speech/speech-hinman-061418>. Further, the speech indicates that a digital asset that was originally offered in a securities offering may later be sold in a manner that does not constitute an offering of a security, in limited circumstances, where: (i) there is no longer a central enterprise being invested in; and (ii) the asset is only being sold to end users who will purchase a good or service available through a network. This also raises a counterfactual question – that is, whether a token network that was once decentralised could “centralise”, such that it would fall within the scope of the securities laws.
8. SEC, Staff Guidance: Framework for “Investment Contract” Analysis of Digital Assets (Apr. 3, 2019), available at <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets> (the “Framework”). SEC, No-Action Letter: Response of the Division of Corporate Finance Re: TurnKey Jet, Inc. (Apr. 3, 2019), available at <https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm> (the “No-Action Letter”).
9. See, e.g., SEC, Press Release: Telegram to Return \$1.2 Billion to Investors and Pay \$18.5 Million Penalty to Settle SEC Charges (Jun. 26, 2020), available at <https://www.sec.gov/news/press-release/2020-146>.
10. See 7 U.S.C. § 1a(9).
11. See 7 U.S.C. § 1a(20) (defining exempt commodity to mean any commodity that is not an agricultural commodity or an excluded commodity; excluded commodity is defined in Section 1a(19) of the CEA to include any “interest rate, exchange rate, currency, security, security index” and other financial rates and assets).
12. See *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015). In this order, the CFTC found that Coinflip’s Bitcoin options were offered in violation of CFTC regulation 32.2, which governs commodity option transactions. The CFTC noted that the options “were not conducted pursuant to [CFTC] Regulation 32.3”, the so-called “trade option exemption”, which permits trading of commodity options on exempt and agricultural commodities, but not on excluded commodities such as securities, currencies, interest rates and financial indices. The CFTC, in describing why the trade option exemption was not available for Coinflip’s options, focused on requirements under CFTC regulation that the options must be offered by eligible contract participants to commercial users of the underlying commodity, and not on the classification of Bitcoin as an excluded commodity.
13. See CFTC Release pr7654-17, CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange (Dec. 1, 2017). See also CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets (Jan. 4, 2018) (describing the CFTC’s authority with respect to virtual currency and the “heightened review” employed during the Bitcoin futures self-certification process).
14. SEC Chairman Jay Clayton, Statement on Cryptocurrencies and Initial Coin Offerings, at n. 2 (Dec. 11, 2017) (“The CFTC has designated Bitcoin as a commodity. Fraud and manipulation involving Bitcoin traded in interstate commerce are appropriately within the purview of the CFTC, as is the regulation of commodity futures tied directly to [B]itcoin.”); see also CNBC, *SEC Chief Says Agency Won’t Change Securities Laws to Cater to Cryptocurrencies* (Jun. 6, 2018) (“‘Cryptocurrencies: These are replacements for sovereign currencies, replace the dollar, the euro, the yen with [B]itcoin,’ Clayton said. ‘That type of currency is not a security.’”).
15. Investment advisers not registered with the SEC may be subject to registration with U.S. states.

16. 17 U.S.C. § 206(4)-2.
17. For an adviser that has its principal office and place of business outside of the United States, an Advisers Act registration exemption is available under the private fund adviser rule, so long as: (i) the adviser has no client that is a U.S. person (generally as defined in Regulation S under the Securities Act) except for “qualifying private funds” (as defined in the rule); and (ii) all assets managed by the adviser at a place of business in the United States are solely attributable to private fund assets with a value of less than \$150 million. Advisers relying on this exemption are still required to file certain information with the SEC.
18. Cold storage refers to the process of storing digital assets, such as Bitcoins, offline (i.e., storing the private keys on a device not connected to the internet). However, the private keys associated with this process may have been exposed to the internet at some time during the generation of the signing process. Deep cold storage, however, is a type of cold storage where not only are the digital assets stored offline, but also the private keys associated with those assets are generated in offline systems, and the signing process of the transactions is also made in offline systems. The systems used in this type of storage never touch the internet; they are created offline, they are stored offline, and they are offline when signing transactions.
19. See 1940 Act § 3(c)(1)-(7).
20. Trevor Kiviat & Gregory Rowland, *The Current State of U.S. Public Cryptocurrency Funds*, *ICLG – Public Investment Funds* (2020 ed.), <https://iclg.com/practice-areas/public-investment-funds-laws-and-regulations/1-the-current-state-of-u-s-public-cryptocurrency-funds> (last visited Aug. 3, 2020).
21. SEC, Staff Letter: Engaging on Fund Innovation and Cryptocurrency-related Holdings (Jan. 18, 2018), available at <https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm> (the “Letter”).
22. See, e.g., SEC Release No. 34-87267; File No. SR-NYSEArca-2019-01 (Oct. 9, 2019), <https://www.sec.gov/rules/sro/nysearca/2019/34-87267.pdf> (last visited Aug. 3, 2020).
23. See CFTC Rule 180.1.
24. 2014-1 C.B. 938.
25. Rev. Rul. 2019-24, 2019-44 I.R.B. 1044.
26. Available at <https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions>. Positions expressed in “FAQs” published by the IRS are not binding authority and may not be cited as precedent in litigation. However, the positions taken in FAQs are helpful because they demonstrate the reasoned views of the IRS with respect to the issues discussed therein.
27. Notwithstanding this seemingly straightforward proposition, the analysis set forth in Revenue Ruling 2019-24 has created confusion among market participants because it refers to “hard forks” and “airdrops” in a manner that does not track those terms’ usage in common industry parlance. Thus, the exact scope of the holdings of Revenue Ruling 2019-24 remains unclear.
28. Under current law, it is not clear whether fork-type income is U.S.- or foreign-source income, or whether it constitutes “fixed determinable, annual or periodical income” (or “FDAP”). Withholding agents, which can include investment vehicles (both partnerships and corporations), are generally required to withhold on and report payments of U.S.-source FDAP to non-resident aliens. The source and character of income can otherwise affect the reporting and withholding obligations of withholding agents as well.

29. Managers may seek to organise funds that are permitted to make loans of digital assets held by the fund in order to generate additional returns for investors in the form of loan fees and interest. While many digital asset loans resemble market-standard security loans, which generally qualify for the non-recognition provision of Section 1058 of the Code (as defined above), it is unclear whether a lender will recognise gain or loss as a consequence of entering into a digital asset loan or as a consequence of the receipt of digital assets upon the termination of a digital asset loan. Despite the existence of strong policy arguments in favour of non-recognition treatment for digital asset loans that resemble market-standard security loans, the risk of triggering taxable gain looms as a possible deterrent to lending activities for funds that are U.S. tax-sensitive.
30. Managers often seek to organise their Offshore Funds or other non-U.S. corporate vehicles in jurisdictions with favourable tax regimes, such as the Cayman Islands or the British Virgin Islands.
31. “Qualifying income” can include income and gain from commodities and income “substantially similar” to income from “ordinary and routine investments to the extent determined by the Commissioner”. *See* IRC § 7704; Treas. Reg. § 1.7704-3.
32. Section 511 of the Code taxes UBTI received by U.S. tax-exempt entities at the rates applicable to corporations or trusts, depending on the relevant entity’s tax classification.
33. If 75% or more of the income of a non-U.S. corporation consists of “passive income”, or if 50% or more (by value) of its assets are “passive assets”, that corporation generally will be treated as a PFIC. *See* IRC § 1297(a). For purposes of the PFIC rules, “passive assets” include assets that do not produce income, and “passive income” includes gain from the sale of passive assets. *See* IRC §§ 1297(a), (b); 954(c)(1)(B)(iii). “Passive income” also includes the excess of gains over losses from transactions in any “commodities” (as defined for purposes of Section 954 of the Code), and therefore any “commodity” as so defined would automatically be a “passive asset”. *See* IRC §§ 1297(a), (b); 954(c)(1)(C). Strong arguments exist for treating certain digital assets as “commodities” for purposes of various Code sections, including Section 954, but this aspect of the taxation of digital assets is likewise uncertain.

* * *

Acknowledgments

The authors gratefully acknowledge Patrick E. Sigmon and Alexander J. Hendin for their assistance in the preparation of this chapter. Mr Sigmon is a partner in Davis Polk’s Tax Department, and Mr Hendin is an associate in Davis Polk’s Tax Department.

**Gregory S. Rowland****Tel: +1 212 450 4930 / Email: gregory.rowland@davispolk.com**

Gregory S. Rowland is a partner in Davis Polk's Corporate Department, practising in the Investment Management Group. He focuses on providing transactional, regulatory and compliance advice relating to investment advisers, mutual funds, closed-end funds, business development companies, private equity funds and hedge funds. He devotes a large portion of his practice to the structuring, launch and operation of registered investment companies and hedge funds and to the sales, acquisitions and restructurings of asset management firms.

Mr Rowland advises financial institutions, technology companies and asset managers in connection with transactional, regulatory and compliance issues concerning digital currency and blockchain activities, including digital currency fund formation. In addition, he advises financial institutions, fund sponsors, corporations, employees' securities companies, and other entities regarding exemptions under the Investment Company Act and Investment Advisers Act.

**Trevor I. Kiviat****Tel: +1 212 450 3448 / Email: trevor.kiviat@davispolk.com**

Trevor I. Kiviat is an associate in Davis Polk's Investment Management Group. His practice focuses on advising clients on the formation and operation of private investment funds, including private equity funds and hedge funds. He also regularly provides regulatory and compliance advice to his private fund clients.

In addition, Mr Kiviat wrote the first widely read and cited academic paper distinguishing Bitcoin from blockchain technology. He advises clients on the novel strategic, operational and regulatory issues relating to digital currency-based businesses, including digital currency fund formation. He also has been cited in the media for his extensive knowledge of blockchain technology and has lectured on related topics at the International Monetary Fund, Duke University and Georgetown University.

Davis Polk & Wardwell LLP

450 Lexington Avenue, New York, NY 10017, USA
Tel: +1 212 450 4000 / Fax: +1 212 701 5800 / URL: www.davispolk.com

Not in Kansas anymore: The current state of consumer token regulation in the United States

David L. Concannon, Yvette D. Valdez & Stephen P. Wink
Latham & Watkins LLP

Developing a framework for consumer tokens

The digital asset sector continues to evolve at a rapid pace. As SEC Commissioner Hester Peirce recently put it, the sector is “about as nimble as it gets.”¹ In 2020, we have witnessed the rise of the decentralized finance, liquidity mining and governance tokens. Non-custodial decentralized exchanges are seeing explosive growth, with their share of total trading volume having grown from less than 1% in June 2020 to over 5% in August 2020, with June, July, and August each representing a record month for decentralized exchange volume.² Non-fungible tokens (NFTs) are gaining traction in the digital art arena, with one piece of digital artwork having sold for approximately \$55,000 in August 2020.³ NFTs are also becoming popular in gaming, with virtual worlds emerging where players participate in virtual economies where they trade property represented by NFTs (*e.g.*, virtual land to build on) for other tokens or labor. We are even beginning to see NFTs being used as collateral to borrow stablecoins and the issuance of tokens that are backed by NFTs.⁴

As the US Securities and Exchange Commission (the SEC) continues to take action with respect to token offerings, the question on the minds of many entrepreneurs and their counsel is what the parameters are for the issuance and sale of “consumer” or “utility” tokens – those designed for use by consumers on a distributed platform and not intended to constitute securities – in the United States.⁵ While there appears to be a viable regulatory path to the issuance of consumer tokens that would not necessarily be viewed as “securities” subject to SEC oversight, the framework remains unclear. In this chapter, we discuss the legal issues surrounding such issuances under the US federal commodities and securities laws.

This chapter serves as an update to the previous edition and reflects our most current and up-to-date thinking and analysis regarding the development of consumer token sales.

Existing frameworks

The securities law framework

The SEC’s approach to whether a digital asset sold in a token sale would be a security derives from its application of the test set forth in *SEC v. W.J. Howey Co.* (the *Howey Test*).⁶ The *Howey Test* determines whether an asset constitutes an “investment contract,” one of the enumerated types of instruments defined in the securities laws.⁷ The test states that an investment contract involves (i) an investment of money, (ii) in a common enterprise, (iii) in which the investor is led to expect profits, (iv) derived from the entrepreneurial or managerial efforts of one or more third parties.⁸ If the test is satisfied, it is immaterial whether the enterprise is speculative or non-speculative, or whether there is a sale of property with or without intrinsic value.⁹ In short, the heart of the analysis is to focus on the economic reality of the arrangement in question.

In July 2017, the SEC applied the *Howey* Test to digital assets for the first time, and arrived at the conclusion that the sale of Decentralized Autonomous Organization tokens (DAO tokens), a digital asset, was an unregistered securities offering undertaken without a valid exemption from Section 5 of the Securities Act of 1933 (the Securities Act). The SEC made clear that to the extent instruments have the indicia of investment contracts, they should be offered and sold in compliance with the securities laws.

In its first enforcement action relating to the sale of digital assets, on December 11, 2017, the SEC issued an order instituting cease-and-desist proceedings to halt Munchee Inc.'s sale of tokens (the *Munchee* Order), having concluded that the sale was an unregistered securities offering. A key lesson of the *Munchee* Order was that despite the utility design features of the MUN Tokens, the manner in which the digital assets were offered to prospective investors, and the presence of investment intent on the part of participating investors, constituted material factors for the SEC in determining that the offering was a securities offering subject to the US federal securities laws.¹⁰

Following the *Munchee* Order, in a June 2018 speech, William Hinman, Director of the SEC's Division of Corporation Finance, emphasized that digital assets need not always be securities. Rather, in addition to the underlying rights associated with such assets, he reiterated that the manner of sale and the reasonable expectations of the purchasers help determine whether a particular digital asset is a security. This is underscored by Director Hinman's reference to *Gary Plastic Packaging v. Merrill Lynch, Pierce, Fenner, & Smith Inc.*,¹¹ in which the court found an offering of a certificate of deposit, which in and of itself is not a security, was subject to US federal securities laws because the issuer's marketing efforts centered on the establishment of a secondary market and the opportunity for purchasers to profit from the enterprise. In the case of nascent token platforms and networks, digital tokens sold in an offering by promoters to "develop the enterprise" will most often constitute securities because the value of the token will primarily derive from the entrepreneurial efforts of the enterprise's promoters. Nevertheless, Director Hinman noted that transactions involving digital assets on a sufficiently decentralized network do not otherwise have the indicia of securities transactions and do not give rise to the public policy concern of informational asymmetries between an investor and issuer, and thus may not trigger the application of US federal securities laws. Director Hinman reiterated these ideas in a May 2019 speech, stating that a potential pathway exists for a token that was once a security to transmute into a non-security. In a February 2020 speech, Commissioner Peirce proposed a token safe harbor, which would provide network developers with a three-year grace period to achieve sufficient decentralization for their network following the issuance of unregistered tokens.¹² Although still a proposal, it is nevertheless a positive development for such a discussion to be taking place.

In April 2019, the SEC staff issued a "Framework for 'Investment Contract' Analysis of Digital Assets" (the Framework) to assist market participants to assess whether a digital asset constitutes an investment contract.¹³ In addition, the SEC staff also released two no-action letters relating to token offerings in 2019. The first (the Turnkey Letter) was in response to a proposed token offering by TurnKey Jet, Inc. (Turnkey Jet), an air carrier and air taxi service, and the second (the PoQ Letter) was in response to Pocketful of Quarters, Inc.'s (PoQ) proposed token offering.¹⁴ Together, the Turnkey Letter, PoQ Letter and Framework emphasize that the analysis of whether a digital asset constitutes an investment contract hinges on the third and fourth prongs of the *Howey* Test; in particular, whether the investors have an expectation of profits that will be derived from the managerial efforts of others. The Framework now serves as the principle source of guidance for analyzing whether a digital asset falls within the definition of a security.

To evaluate “reliance on the efforts of others,” the Framework introduces the concept of an Active Participant (AP), defined as “a promoter, sponsor, or other third party ... [that] provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profit from those efforts.” Determining the existence of an AP necessarily requires an analysis of each party’s role in developing, maintaining or governing the network. The presence of an AP means it is more likely that profits are being derived from the efforts of others.

To analyze “reasonable expectation of profit,” the Framework bases its evaluation on whether an asset conveys the “right to share in [an] enterprise’s income.” This factor should be unsurprising to issuers, as it derives from the reasoning in the *DAO Report*, which pointed to the dividend-like feature of DAO tokens in classifying them as securities. Continuing in the vein of the SEC’s prior pronouncements, the guidance also looks to how the digital asset is marketed, whether “the digital asset is offered broadly” (e.g., via secondary markets) “to potential purchasers as compared to being targeted to expected users of the goods or services or those who have a need for the functionality of the network,” and whether “[t]he AP continues to expend funds from proceeds or operations to enhance the functionality or value of the network or digital asset.” Such factors appear to focus on the more speculative aspects of issuances, such as where the use and value of the digital asset is connected to an undeveloped network, the success of which may likely be tied to the capital raised through the issuance itself. In addition, the Framework looks to whether the AP will receive or retain any of the digital assets, and the nature of purchasers’ expectations with respect to the role of the AP and the ongoing viability of the digital asset itself.

In June 2019, the SEC sued Kik Interactive Inc. (Kik) for allegedly conducting an illegal \$100 million securities offering of Kik’s digital token, Kin.¹⁵ In its complaint, the SEC alleged that Kik marketed Kin to investors as an investment opportunity, offered and sold Kin before it had any utility, retained a proportion of the tokens for Kik and promised investors that Kin would be listed on secondary markets. For the SEC, such features meant the Kin offering was a securities transaction and should have complied with registration requirements as prescribed by the securities laws.¹⁶ In a press release,¹⁷ Kik responded to the SEC’s suit, citing similar arguments as those raised in its Wells submission¹⁸ in December 2018. Specifically, Kik argued that the SEC’s complaint is based on “flawed legal theory” and expands the *Howey* Test beyond its proscribed limits. In support of this position, Kik claimed that “the complaint assumes, incorrectly, that any discussion of a potential increase in value of an asset is the same as offering or promising profits solely from the efforts of another; that having aligned incentives is the same as creating a ‘common enterprise’; and that any contributions by a seller or promoter are necessarily the [‘]essential[’] managerial or entrepreneurial efforts required to create an investment contract.”¹⁹ Of course, in addition to proving instructive, the resolution of this case and these issues could provide useful judicial precedent.

In June 2020, a year after commencing the Kik lawsuit, the SEC announced a settlement with Telegram Group Inc. (Telegram) over charges that Telegram had violated securities laws when it offered and sold its unregistered “Grams” token in exchange for \$1.7 billion from 175 initial purchasers.²⁰ The Telegram fact pattern is strikingly similar to Kik’s, in that both are operators of messenger applications that sought to introduce a token into their messenger service by selling pre-functional tokens to initial purchasers and using the funds to develop their respective networks.²¹ Prior to the settlement, the Court in the Southern District of New York had sided with the SEC in March 2020 and granted an injunction prohibiting Telegram from delivering Grams to the initial purchasers. The Court held that Telegram’s scheme

constituted an investment contract, requiring either registration or an applicable exemption in order to comply with securities laws. As part of the settlement with the SEC, Telegram returned \$1.2 billion to the initial purchasers and paid an \$18.5 million penalty.

Some commentators had hoped Telegram's case would provide further clarity on the path tokens should take to not constitute securities. Unfortunately, those hopes were not met, but the Court provided a brief hint of what might be, noting:

“Cryptocurrencies (sometimes called tokens or digital assets) are a lawful means of storing or transferring value and may fluctuate in value as any commodity would. In the abstract, an investment of money in a cryptocurrency utilized by members of a decentralized community connected via blockchain technology, which itself is administered by this community of users rather than by a common enterprise, is not likely to be deemed a security under the familiar test laid out in [*Howey*]. The SEC, for example, does not contend that Bitcoins transferred on the Bitcoin blockchain are securities.”²²

The commodities law framework

The US Commodity Futures Trading Commission (the CFTC) regulates the swaps (*i.e.*, the CFTC's term for derivatives) and futures markets and retains general enforcement authority to police fraud and manipulation in cash or “spot” commodities markets.²³ In 2014, then-CFTC Chairman Timothy Massad observed that what the CFTC has referred to as virtual currencies are “commodities” subject to provisions of the Commodity Exchange Act, as amended (the CEA).²⁴ Since 2015, the CFTC has been active in bringing enforcement actions when virtual currency enterprises run afoul of regulatory requirements²⁵ and in the enforcement against fraud and manipulation in the virtual currency “spot” markets.²⁶

The CFTC also regulates certain retail commodity transactions that are leveraged, financed, or margined as if they were futures. The developing crypto spot markets have increasingly seen use of leverage and margin for trading of crypto-assets. The CFTC recently finalized interpretive guidance (Guidance) on what constitutes “actual delivery” in the context of crypto-assets that serve as a medium of exchange (*i.e.*, virtual currency). Under the CEA and CFTC regulation, commodity transactions with retail customers that are leveraged, margined or financed are subject to regulation as futures contracts by the CFTC unless an exemption applies (the Retail Leveraged Commodity Rules). If the commodity (*i.e.*, virtual currency) is delivered within 28 days, such leveraged transaction will not be subject to regulation as a futures contract. The Guidance provides two primary factors for what would constitute “actual delivery” for purposes of the Retail Leveraged Commodity Rules: first, the purchaser must have possession and control over the virtual currency; and second, the purchaser must be able to use the virtual currency in commerce.

Pre-functional consumer token sales²⁷

Sales of tokens to fund an AP's development of a token-based network have long been considered to constitute investment contracts, regardless of the form of instrument evidencing the sale. That is, the efforts of the AP remain central to the value of the instrument being sold, thus satisfying the *Howey* Test as an investment contract. As a result, in an effort to separate the pre-functional sale and the underlying consumer token, new financing instruments – including the Simple Agreement for Future Tokens (the SAFT)²⁸ and other similar token presale instruments – were designed. While such instruments attempted to solve the securities law issues with presales, they raised other significant concerns.²⁹

Securities law issues

Token presale instruments commonly fail to address the status of the underlying tokens and the impact of the presale offering on the marketing of the underlying tokens. That is, by marketing the token presale as an investment opportunity, these instruments were implicitly marketing the investment value of the underlying token. As a general matter, such instruments have been and continue to be marketed to purchasers with investment intent, such as hedge funds, venture capital funds and others, and, in at least some cases, purchasers are required to represent that they are purchasing for investment purposes.³⁰ In addition, settlement of these instruments contemplates delivery of the token at network launch,³¹ and thus, at least with respect to the initial iteration of these instruments, the delivery of tokens for consumptive use will occur contemporaneously, or at least nearly so, with the delivery of tokens to purchasers who were investors. This would seem to argue in favor of the proposition that a token launch with delivery of tokens in settlement of these instruments is not directed solely to consumers, and, under the logic of *Gary Plastic* and the *Munchee* Order, is a securities transaction, not a consumer token launch.³²

While recent iterations of these instruments have begun to acknowledge that issuances of the underlying tokens could be securities transactions, they continue to subject issuers and purchasers to significant risks by potentially increasing the likelihood that the underlying tokens will be deemed to be securities. This does not represent a viable outcome for many token-based networks, which require the free transfer of tokens on the network as part of their necessary function, because the US securities laws often require the existence and registration of an intermediary in securities transactions (*i.e.*, the transfer of tokens deemed to be securities). Accordingly, an issuer or platform may be required to register as a broker-dealer or exchange (or alternative trading system)³³ to permit the functioning of its token-based network,³⁴ which would render many token-based networks unusable. Although recent statements indicate an acceptance of the notion that a digital asset originally issued as a security could subsequently cease to be a security once the network is sufficiently decentralized,³⁵ the uncertainty that remains regarding the viability and timing of the consumer token sale raises challenges for appropriate disclosures to investors and potential liability for issuers. This is particularly the case when the entire investment decision is based on the availability and functionality of the underlying token, and it would seem to be challenging to craft sufficient disclosure in such a circumstance where the entire investment proposition is subject to this level of uncertainty.

Recent examples of the unintended consequences of using token presale instruments can be seen in the SEC's actions against Kik and Telegram.³⁶ Kik and Telegram each offered and sold pre-functional tokens to accredited investors in private placements pursuant to Regulation D via token presale agreements. Despite this, the SEC's view was that the private nature of the sales of tokens under the token presale instruments was vitiated because these sales were part of schemes that involved token sales to the public and thus constituted a single plan of financing that did not qualify for the private placement exemption from registration under US securities laws. In its Kik complaint, the SEC noted that "Kik sold the Kin as part of a single plan of financing, for the same general purpose, at about the same time, without creating different classes of Kin[.]"³⁷ Similarly, in halting the delivery of Telegram tokens to the initial purchasers, the Court found that "the delivery of Grams to the Initial Purchasers, who would resell them into the public market, represents a near certain risk of future harm, namely the completion of a public distribution of a security without a registration statement."³⁸

Commodities law issues

Beyond the securities law concerns, the SAFT, and other similar token presale instruments, also raise commodities laws concerns. Because cryptocurrencies are commodities,³⁹ a presale of consumer tokens through an instrument that provides the right to receive tokens in the future, or confers the right to exchange or convert such instrument into tokens that are not securities, may be a forward contract for the sale of a commodity or a commodity option, and subject to regulation by the CFTC as a swap, if an exemption is not available.

(a) Commodity forward contracts

Forward sales of commodities fall within the CEA's broad definition of "swap," which encompasses numerous types of derivatives, and are subject to regulation by the CFTC absent an applicable exclusion.⁴⁰ Notably, the sale of a non-financial commodity for deferred shipment or delivery is excluded from the swap definition, so long as it is intended to be physically delivered,⁴¹ but provided such forward contract also qualifies as a commercial merchandising transaction (Non-Financial Forward Contract Exclusion).⁴² If such instruments are purchased by investors or speculators, they will not satisfy the requirement of the Non-Financial Forward Contract Exclusion because the purchasers are not "commercial market participants."⁴³ The CFTC has expressly stated that hedge funds, acting in their capacity as investors, are not commercial market participants.⁴⁴ As such, token presale instruments are effectively a prepaid forward contract of a commodity whereby parties have agreed a price or percentage discount on the token to be delivered at a later date. As discussed above, the many token presale agreements are (and continue to be) largely marketed to investors and not commercial market participants;⁴⁵ such investors would not be eligible for the Non-Financial Forward Contract Exclusion.

(b) Commodity options

More recent versions of token presale instruments have also included convertible features, which provide investors or the issuer, as applicable, a call or put right to deliver tokens upon the consummation of a token sale at an agreed price or discount. Such an instrument may constitute a commodity option and would be subject to CFTC regulation as a swap,⁴⁶ unless an exemption applies. Trade options are generally exempt from regulation by the CFTC, other than certain large trader reporting requirements and the CFTC's general anti-fraud and anti-manipulation enforcement authority (the Trade Option Exemption).⁴⁷ In order to qualify as a trade option and benefit from the Trade Option Exemption,⁴⁸ the commodity option in question must be: (i) intended to be physically settled if exercised; (ii) entered into with an offeror who is either an eligible contract participant (ECP)⁴⁹ or a producer, processor or commercial user of, or merchant handling, the commodity (or products or by-products thereof) that is the subject of the option, and such offeror is offering to enter into such option solely for the purposes related to its business as such; and (iii) entered into with an offeree who is either a producer, processor or commercial user of, or merchant handling, the commodity (or products or by-products thereof) that is the subject of the option, and such offeree is entering into such option solely for the purposes related to its business as such.

Unfortunately (as stated above in connection with the Non-Financial Forward Contract Exclusion), many of the token presale instruments are not offered to commercial market participants who would satisfy the "offeree" prong, even if the issuer of the instrument could satisfy the "offeror" prong. Additionally, even if such instruments are offered to "consumers," they would not necessarily satisfy the "offeree" prong of the Trade Option Exemption, unless such consumer could establish a nexus to a business activity. Accordingly, token presale investors are unlikely to qualify for the Trade Option Exemption.

(c) *Hybrid Instrument Exemption*

Furthermore, since token presale instruments may constitute or contain a commodity forward contract or commodity option and may not otherwise qualify for the Trade Option Exemption or the Non-Financial Forward Contract Exclusion, we also consider whether such instruments would meet the Hybrid Instrument Exemption (defined below) and, as a result, be exempt from commodities law regulation. Under CFTC Rule 34.2(a), a “hybrid instrument” is defined to include an equity or debt security with “one or more commodity-dependent components that have payment features similar to commodity futures or commodity options contracts or combinations thereof.”⁵⁰ Under Section 2(f) of the CEA, a hybrid instrument that is “predominantly a security” is exempt from the provisions of the CEA if, among other things, the instrument is not marketed as a contract of sale of a commodity for future delivery (or option on such a contract) subject to the CEA (the Marketing Condition) (such exemption being the Hybrid Instrument Exemption).⁵¹

While token presale instruments may, in theory, be capable of qualifying for the Hybrid Instrument Exemption, because they are often primarily marketed to investors who themselves are solely or in large part motivated to purchase such instruments in order to receive the underlying commodity (*i.e.*, the token), such instruments will often fail to satisfy the requirements of the Marketing Condition of the Hybrid Instrument Exemption.⁵²

(d) *Retail leveraged transactions*

Further still, under certain structures, network participants who are also functionally retail investors may wish to receive a token. Network participants may receive such tokens through the financing of a third party or the network platform itself. The recently issued Guidance with respect to Retail Leveraged Commodity Rules has clarified uncertainty over what delivery actually means in this context and stresses meaningful possession and control and the ability to use such token in commerce. In certain instances, neither utility nor control is practicable within a 28-day timeline. As a result, such token pre-sale structures may be regulated as futures contracts.

(e) *Consequences of CFTC regulation*

Because such presale instruments may have an embedded swap, which does not qualify for an exemption from regulation by the CFTC (as discussed above), such presale instrument would be subject to the full swaps regulatory framework applicable to such instruments, or in the case of Retail Leveraged Commodity Rules, subject to regulation as a futures contract. In particular, in order to trade over-the-counter, swaps must be entered into between ECPs.⁵³ While some investors may qualify as ECPs, token issuers typically are early-stage companies that may not have at least \$10 million gross assets, and as a result, would not satisfy the ECP test. A swap entered into by parties who are not ECPs would be in violation of the CEA and CFTC regulation. As a result, the contract could be rescinded and both parties could face penalties and sanctions for such actions.

Potential solutions available through traditional financing instruments

Traditional early-stage financing structures, such as preferred stock and convertible promissory notes,⁵⁴ are “tried and true” structures that generally exhibit the necessary flexibility to address the needs of early-stage companies/token issuers and token platforms. We believe these structures can be augmented to address investor demand for exposure to consumer tokens, while enabling the parties to comply with applicable securities and commodities laws. This can be achieved by providing investors with various combinations of token-related purchase, economic and voting rights.

First, the conversion and exchange rights featured in currently popular token presale instruments could be replaced with appropriately limited token sale participation and economic rights that reduce the regulatory risks associated with consumer token sales discussed above. For instance, the purchase right would not represent a conversion or exchange of the security, but would include these rights in addition to the rights granted to the holder of the securities. The exercise of such token sale participation rights could be limited to sales or distributions of the consumer tokens that would not be deemed to be securities transactions, such as when the network had achieved sufficient decentralization (although the challenges in defining an objective standard for this trigger may reduce the practicality of this option). The participation rights could also be limited to purchases for actual use, or limit the consumer tokens reserved for distribution or sale to investors, and require that any distributions or sales thereof occur in a manner that supports the broader consumer token-based network.

Instead of the inclusion of pre-negotiated token prices in such instruments, which – from a commodities law point of view – may increase the risk of being considered a commodity option because such pre-agreed price could be seen as a strike price, the participation rights could be coupled with “most-favored nation” (MFN) pricing provisions, guaranteeing certain investors the best token sale and distribution terms offered by the issuer to any other third party. These rights could also be supplemented with token economic rights that could be triggered *in lieu* of participation in the consumer token sale. For example, preferred stock could be issued with various rights tied to consumer token sales, such as pre-negotiated dividend or redemption rights, or a convertible promissory note under which the issuer pays a multiple of the note’s aggregate principal amount or the note converts into preferred stock with dividend or redemption rights. Such token economic rights would have the goal of providing the investor with a similar economic outcome of participating in the consumer token sale. As a result, the careful balancing of such token sale participation and economic rights could provide issuers the flexibility to allow for the participation of investors eager to receive token economics while protecting the development of the underlying network and consumer tokens from the application of the securities laws.

Second, because consumer tokens and the corresponding network protocol often represent a significant portion of the value proposition associated with investing in such platforms, investors can reasonably expect to receive voting rights with respect to the creation and distribution of tokens by the issuer, including the right to approve the initiation of any offerings or distributions.⁵⁵ Eventually, as the pathway for consumer token sales becomes clearer, voting rights grants may be more narrowly tailored to only apply when such a sale does not meet certain specifications. In addition, investors may seek additional protections to prevent potential uses of the issuer’s token-based network that circumvent their consumer token-related economic and participation rights.

Finally, these preferred stock and convertible promissory note structures may also be preferred from a commodities law perspective for several reasons. First, conferring future participation rights on an investor to participate in a token sale, or conferring economic rights to an investor in respect of future distributions, is not clearly a swap under the CEA and subject to CFTC regulation. Currently, no regulatory certainty exists as to the treatment of preferred stock and convertible promissory note structures with token participation rights, and it is unclear whether such participation rights would constitute swaps (or not) subject to CFTC jurisdiction. There is no strike price or final price differential that creates market risk that the CFTC would necessarily be incentivized to regulate in the commodity options market. Such token participation rights seek to reduce economic risk and loss attributable

to other token presale agreements. They afford the investor an MFN pricing provision to purchase the token at spot price, which is likely to reduce an investor's risk of loss. Accordingly, for the reasons set forth above, we believe such structures reduce regulatory risk of CFTC intervention which is inherent in predecessor token presale instruments.

Second, if a swap were deemed to exist, in such structures where the conditions of the Hybrid Instrument Exemption other than the Marketing Condition are satisfied, one could argue that – despite the associated consumer token rights – such instruments are “predominantly securities” and unlikely to run afoul of the Marketing Condition, because the commodity forward or option would be a small portion of the value of the instrument. Accordingly, it would be much harder to argue that such instrument was marketed as a swap or purchased by investors solely for the purpose of receiving the value provided by the swap component. That is, because the predominant value of the instrument is a traditional security providing specific rights with respect to the issuer – such as traditional preferred stock rights (e.g., liquidation preference, dividends, anti-dilution protection) or traditional promissory note rights (e.g., returns of principal, potential conversion into equity) – such consumer token presales could arguably fall outside some (if not all) of the CFTC regulatory regime by qualifying for the Hybrid Instrument Exemption or being excluded entirely from the swap definition.⁵⁶

Of course, while each instrument would need to be analyzed on its own merits, we believe these alternate structures have great promise for addressing commodities law issues. At minimum, they significantly mitigate the regulatory risks of the SAFT and other similar presale token structures; and at best may offer a clear path to avoid characterization as a swap subject to CFTC jurisdiction.

Importantly, even if these preferred stock and promissory note structures are not completely exempt from regulation as a swap, certain token projects and network participants may qualify for the Trade Option Exemption, giving further relief from CFTC regulatory requirements.

These structures are also preferred from a securities law perspective for many similar reasons – because the investor is receiving a more traditional security, the various rights they are purchasing are far less ambiguous, and appropriate disclosures regarding the material aspects of the investment are more easily crafted.

Please note that in collaboration with ConsenSys, we have offered up a convertible note tool which we believe addresses the concerns raised in this chapter.⁵⁷

Enabling true consumer token sales

Once a platform and token protocol have been developed, the question remains whether a viable consumer token sale may be accomplished. The Framework identifies a number of factors centering around two main inquiries to help distinguish when digital assets transactions may be characterized as securities transactions.⁵⁸ First, the Framework emphasizes the necessity of the AP for the continued success of the enterprise. Second, the Framework emphasizes the expectations held by network participants with regard to the AP and the token. Critical in this inquiry is the nature of the marketing of the consumer token and its platform, and the nature of the purchasers.

We believe we can draw three concrete takeaways from the Framework that bear upon this analysis. First, tokens offered in a manner intended to appeal to an investor's investment intent will trigger the application of the securities laws. Second, when the token-based network has developed to an extent that the value of the tokens is no longer dependent

upon the entrepreneurial or managerial efforts of such network's APs, token trading on that network will not be considered securities transactions. Third, offerings of tokens with utility on a functioning token-based network that are specifically directed solely to users of that network may be conducted in a manner that renders the securities laws inapplicable.

Features of established non-security virtual currencies

Two of the most widely held and well-known digital assets – Bitcoin and Ether – provide good examples of digital assets that Director Hinman expressly posited no longer constitute securities primarily due to the decentralized nature of their use.⁵⁹ The “efforts of others” prong of the *Howey* Test requires that such efforts must be “undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise.”⁶⁰ Two seminal cases provide guidance on this prong for instruments traded in well-developed markets such as Bitcoin and Ether.⁶¹ In both *Noa v. Key Futures* and *SEC v. Belmont Reid & Co.*, the Ninth Circuit applied the *Howey* Test to the sale of precious metals, finding that the *Howey* Test is not satisfied if the expectation of economic return is based on market forces, and not on the efforts of an AP. Thus, the applicability of these cases to the analysis of Bitcoin and Ether within this prong of the *Howey* Test (and therefore the analysis of whether either Bitcoin or Ether is a security) depends on the existence of an established, decentralized market where the spot price is determined by ordinary market forces.

What is the role of the AP? Decentralized networks

As discussed above, the SEC's emerging regulatory framework for consumer tokens appears to be focused on a threshold question derived from the fourth prong of the *Howey* Test: Is the token-based network sufficiently decentralized/independent of the entrepreneurial efforts of the AP? There are several factors underlying this inquiry and each case requires careful analysis, and, without further guidance from the SEC, it is difficult to predict the appropriate weighting of such factors.

(a) Ongoing development and maintenance of the network

For a token-based network to be truly decentralized, no AP should have the ability to significantly and directly influence the value of the consumer tokens exchanged on the network. This implicitly includes ongoing efforts to develop and maintain the network. The Framework states it is more likely that a token purchaser is relying on the efforts of others if “[a]n AP is responsible for the development, improvement (or enhancement), operation, or promotion of the network, particularly if purchasers of the digital asset expect an AP to be performing or overseeing tasks that are necessary for the network or digital asset to achieve or retain its intended purpose or functionality.” Open source projects, where a variety of parties may contribute to the ongoing development of the network, clearly have a greater chance of meeting this requirement.

(b) Use of token sale proceeds

Similarly, the expected use of proceeds from a related token sale can impact whether a related token-based network is sufficiently decentralized. For example, a use of proceeds that involves further development and maintenance of the network could lead to a conclusion that the efforts of the issuer remain central to the value of the token. The Framework states that reasonable expectation of profits is more likely to be present if “[t]he AP continues to expend funds from proceeds or operations to enhance the functionality or value of the network or digital asset.” This further supports the use of traditional financing instruments, coupled with economic rights in future token offerings. Issuers utilizing such instruments would be able to fund the development of their network from the investments received pursuant to such instruments and would,

subsequently, be able to use the proceeds from token sales to deliver a return of capital to investors, thereby clearly distinguishing early-stage investments from token purchases and supporting the position that the tokens themselves should not be deemed to be securities.

(c) *Network governance*

The Framework also indicated that a token-based network's governance structure will be considered when determining whether such network is decentralized.⁶² In its most simple form, a decentralized governance structure would provide token holders the ability to directly determine matters relevant to the network's development. Reliance on the efforts of others is more likely to be deemed present if an AP has a continuing managerial role in network governance, including exercising judgment concerning the network or the characteristics and rights that the digital asset represents. The sufficient decentralization argument is strengthened if the AP can avoid playing a lead role in making decisions regarding governance issues, code and protocol updates, and how third parties participate in the validation of transactions that occur with respect to the digital asset.

(d) *Robust token economy*

The value of tokens on certain token-based networks is driven by a robust token economy pitting a number of different forces with different operating incentives against each other. These competing elements will be ascendant, and have a corresponding impact on the token value, at differing times. Courts have reasoned that this sort of market valuation mechanism is critical to distinguish a commodity from a security, as the value in the instrument is created by these broad market forces rather than the efforts of others.⁶³ The Framework also recognizes this principle, noting that token "[p]rice appreciation resulting solely from external market forces impacting the supply and demand for an underlying asset generally is not considered "profit" under the *Howey* test." Filecoin⁶⁴ is an apt example of a robust economic structure that helps ensure market forces drive token values independent of the AP's efforts. The Filecoin network involves three network participants: (i) clients, who pay to store and retrieve data; (ii) storage miners, who provide data storage to the network; and (iii) retrieval miners, who provide data retrieval to the network.⁶⁵ As a result, the competing activities of these three groups create the value of a Filecoin token through the creation of supply and demand economics. This also means the success of the Filecoin network hinges upon a sufficient number of market participants contributing to the network simultaneously, which is a premise reflected in the high proportion of Filecoin tokens allocated to miners in exchange for storage and retrieval services.⁶⁶

There are numerous token-based networks and token economy models that similarly promote the development of a robust economic structure. The success of most decentralized token-based marketplaces, whether for data storage, digital assets in virtual worlds, artificial intelligence, real estate or intellectual property, is dependent on market participants driving the value of the networks and its corresponding tokens. As a result, these marketplaces, like those for Bitcoin and Ether (which rely on market participants to record transactions on their respective blockchains), have a market valuation mechanism that is helpful in distinguishing a commodity from a security.

Is the asset designed for consumptive purposes? Consumer tokens and consumer token sales

Numerous consumer token and consumer token sale features warrant consideration in furthering the consumer token analysis to determine whether the securities laws may apply.

(a) *Functioning network*

A factor closely related to the role of the AP, though distinct, is the question of whether the token-based network is "fully functioning or in the early stages of development."⁶⁷

A common feature of many early token sales was that they were commenced before the consumer could actually utilize the token. While some consumer goods are purchased in this manner (e.g., concert tickets or a new Tesla car), consumer token presales complicate the analysis of whether “the primary motivation for purchasing the digital asset is for personal use or consumption.”⁶⁸ Although it remains difficult to assign weighting to the factors presented in the Framework, network functionality appears to be a factor that has significant bearing. As such, issuers should, to the extent possible, launch their token-based network prior to initiating consumer token sales.

(b) *Secondary markets and transferability*

In February 2018, SEC Chairman Jay Clayton testified before the US Senate Committee on Banking, Housing and Urban Affairs, in part sharing his particular concern for token issuers and emphasizing the secondary market trading potential of the tokens offered for sale.⁶⁹ This line of thinking clearly follows the *Gary Plastic* case, where the marketing of a non-security investment (i.e., bank certificates of deposit) that included the promise of a secondary market transmutes the certificates of deposit into investment contracts.⁷⁰ Accordingly, the Framework states that if the AP promises to arrange trading of the digital asset on a secondary market, this means the token purchasers reasonably rely on the AP for liquidity, strongly supporting the view that such token is a security. However, the mere availability of a secondary market developing following a token sale arguably should not be dispositive and, perhaps, should not matter at all. Again, *Gary Plastic* stands for the notion that it is the *marketing* of the “investment” based on the potential of the secondary market that is what makes the instrument a security. Of course, there are many everyday commodities for which secondary markets regularly develop – in fact, eBay has built a robust business on this basis – and the mere existence of such markets does not transmute the instruments into securities.

For example, a large number of active market participants is critical to the success of Filecoin’s network. It is difficult to imagine a scenario where it could achieve the critical mass of network participants necessary if such network participants were restricted from exchanging in some way their Filecoin tokens with other participants for other digital assets or tokens as part of continually broadening the universe of token holders. In order for a network to work under isolated conditions, where such transfers were not permitted, not only would suppliers have to consume the resources created by the network, but maintaining a balance among suppliers and producers would be exceedingly difficult. The secondary market transactions accordingly act to balance the various economic demands without any one actor having to play all roles. Otherwise, for Filecoin, a miner would need to both provide and consume storage and retrieval services, because consumption would be the only way to realize the economic gain in exchange for providing such services. As a result, there would be little incentive for the miner to participate on such a network. A similar case can be made for any network that includes both suppliers/producers of goods or services and consumers of goods or services. Furthermore, supply on any such market would decrease rapidly if the inputs required to produce the supply of goods and services were not principally derived from the tokens received upon sale, or if an insufficient number of other goods and services were available to enable suppliers to consume all of the tokens they earn within such marketplace. Given the negative effect on network participation that limiting secondary market activity would have, it is likely that overly broad restrictions would impede competition and that only the largest and most established marketplaces would succeed. Because of the foregoing, a measured approach to addressing secondary market activity and transferability is advisable. Fortunately, the flexibility arising out of ongoing

innovation in blockchain technology provides companies with several options. First, purchasers of consumer tokens in a consumer token sale could be required to agree to a lockup mechanism, whereby a smart contract prevents the purchaser from selling their tokens for a certain period of time or until they participate on the network in the required manner. The purchaser's tokens could be unlocked initially only in the event they were utilized on the platform itself first, and thereafter could be traded in the secondary market. Second, a tiered transfer fee or other incentive structure could be implemented, whereby the fees (or other similar incentives) for tokens transferred in connection with participation on the token-based network could be lower than the fees for transfers to non-network participants. In each of these cases, initial purchasers would not have the same profit motive in seeking secondary market for token sales as they may have in a typical token offering.

Director Hinman appears to have suggested as much in his enumerated factors.⁷¹

(c) *Inflationary issuances*

Another aspect of consumer token sale structures that warrants discussion is the impact of inflationary/deflationary pressures in token economies. Depending on the token structure, there are a number of scenarios in which subsequent issuances of tokens in exchange for contributions to the economy of the network can simultaneously facilitate network growth while limiting the immediate speculative potential of the token. For example, Filecoin's token allocation design made 70% of the total Filecoin tokens available for miners in exchange for data storage and retrieval services. As those tokens will be subsequently distributed and "earned" by miners, the Filecoin token purchasers are "diluted" in an inflationary sense. However, unlike in the context of an equity security where dilution is significant because the valuation of the interest is always proportionate to the relative interest in the enterprise value, here the value of the token is based on the value of the goods and services that may be received in exchange, and the market supply and demand for such goods and services. Thus, the impact of dilution on a true consumer token is quite different and the value of the token should correspond more directly to the value to the consumer of the applicable goods and services. As a result, consideration should be given to the supply dynamics of a token economy.⁷² Ultimate control over dilutive issuances is also a factor in network governance, which may impact the analysis above regarding the decentralization of a given network.

(d) *Token retention*

To date, a common feature of token offerings has been the retention of the tokens by issuers for distribution to founders, employees, advisors and investors. In instances where there are reasonable and justifiable grounds to believe that these individuals can and will consume these tokens through their own market participation and will thus assist in the seeding of the network, then consumer token issuers should not be dissuaded from including the retention of consumer tokens in their allotment strategy. However, issuers should exercise caution in doing so, particularly in cases where the products and services offered on an issuer's network or the number of tokens retained could not reasonably be consumed by its founders, employees, advisors and investors. In such instances, it would be difficult to make a credible argument to the SEC that such tokens are not being held for investment purposes.⁷³ The Framework states that token retention by an AP cuts towards reliance on the efforts of others given that token "[p]urchasers would reasonably expect the AP to undertake efforts to promote its own interests" by taking actions that enhance the value of the digital asset. In addition, such retention of tokens also makes it more difficult for the token issuer to demonstrate

that the tokens are “[d]ispersed across a diverse user base[,]” rather than being “[c]oncentrated in the hands of a few that can exert influence[.]”⁷⁴

As a result, companies who wish to reward their teams for the successful development of a token-based network giving rise to a consumer token sale should look to traditional equity compensation methods, which can be augmented by consumer tokens to the extent a viable use case can be established. Additionally, selling restrictions with respect to both timing and price of tokens by such holders could be adopted to bolster the argument that such grants were not made to persons with an investment intent.

(e) *Virtual currency peg/stablecoins*

Another means of limiting the speculative potential in the purchase and sale of consumer tokens could be the adoption of token structures that initially peg the value of the consumer token to fiat or virtual currency, also known as a “stablecoin.” The Framework highlights that tokens designed and marketed as virtual currencies are less likely to be considered securities under the *Howey* Test if the token can be used to pay for goods or services without first having to convert it to fiat currency or another token. In addition, the token must operate as a store of value that can be saved, retrieved, and exchanged for something of value at a later time. In the Turnkey Jet matter, the company alerted the SEC of its intent to issue “tokenized jet cards” (tokens) on a user platform facilitating the procurement of chartered airline flights. In its letter to the SEC, Turnkey Jet made clear that consumers of these tokens would be “motivated . . . by a desire to obtain on-demand air charter services,” not by an expectation of future profits. Accordingly, Turnkey Jet maintained that these tokens would not be securities under the *Howey* framework. The SEC agreed, and identified several key attributes of the Turnkey Jet tokens that highlighted their consumptive utility and non-speculative nature. Specifically, the Turnkey Letter noted that Turnkey Jet’s tokens would be immediately usable, have a fixed value of one USD per token and would be marketed in a manner that emphasized their functionality and not the potential for an increase in their market value. Similarly, in issuing the PoQ Letter, the SEC noted that PoQ’s token having a fixed price factored into its considerations.⁷⁵

As an alternative, in the case of an early-stage marketplace, an issuer could incentivize sellers to advertise their products or services in both the network’s native virtual currency/token, as well as, for example, Ether, with the price of the goods or services being determined by the market price of Ether. The transaction could then be consummated in the native token of the network. This structure could have the effect of deterring speculative purchases at the time of an issuer’s consumer token sale because the price of the token would presumably face downward pressure to remain in line with the exchange rate with the virtual currency peg. As a result, a virtual currency peg could result in the price of a given consumer token being primarily influenced by individuals or events beyond the token issuer’s control and may therefore be viewed favorably by the SEC.⁷⁶ Once a larger and more functional network was operational with APs, these incentivizing schemes could be removed to allow for free market activity.

We would note that stablecoins may be swaps subject to CFTC regulation. Such structure would need to be carefully considered under commodities laws.

(f) *Token sale legal documentation*

Another means of discouraging purchasers of consumer tokens from an expectation of profit could be found in the documentation used in sales of tokens by issuers. Such agreements could include representations and warranties requiring purchasers to state that their intention is to use such consumer tokens on the issuer’s network.

As discussed above, such documentation could also include lockup mechanisms, whereby the purchaser's tokens could be "locked" using a smart contract for a specified period. Furthermore, instruments could grant issuers a first refusal with respect to any purchaser's tokens, whereby the issuer would be entitled to repurchase the tokens held by a user if the user had determined not to use them on the issuer's network. In many respects, this could be functionally similar to rights of return that are commonly provided by retailers with respect to tangible consumer goods, and issuers may be well advised to allocate a small percentage of any consumer token sales for such repurchases. While on most networks the issuer will only ever have privity of contract with the initial purchasers of consumer tokens, utilization of these mechanisms could substantially reduce the risk of such purchasers having an expectation of requiring the protection of securities laws. However, establishment of valuation protocols and resale price, as well as the potential of a withdrawal of cash from an issuer, may detract from the attractiveness of this alternative.

Seeding network activity and achieving decentralization

Based on the foregoing considerations, issuers who both operate decentralized networks featuring tokens designed for consumption, and sell such tokens in a manner designed to dissuade purchases for investment, should be capable of avoiding the application of securities laws to such token sales under the *Howey* Test. However, this current paradigm appears to create a paradox, given that the process of creating a decentralized and functional network on which consumer tokens can be utilized necessitates that issuers first seed network activity by issuing consumer tokens in transactions that do not trigger the application of the securities laws.

As a result, issuers may seek to seed their network through the distribution of consumer tokens via "airdrops" and other distributions to affiliates, vendors and community members. Such distributions promote network activity, facilitate the implementation of governance procedures and enable network testing prior to full launch. The information garnered from this process enables developers to resolve potential issues and simultaneously enhances the credibility of the project both within and outside its community. Furthermore, such activity can help consumers better understand the value of the overall network and each consumer token, which ultimately promotes market efficiency. The benefits of such seed activity extend to consumer token issuances targeting strategic partners, who may also assist with the development of the network prior to launch. In addition, this seed activity permits the nascent token economy of the platform to grow, allowing forces beyond those of the initial AP to begin to determine the value of the token. As a result, this activity directly addresses several of the factors identified by Director Hinman and can strengthen the case that a particular token is a consumer token.⁷⁷

Nonetheless, issuers need to be aware that the SEC takes the view that the securities laws apply to airdrops of tokens, even though no money or digital currency funds are given by airdrop recipients. For example, in the early days of the internet, some issuers sought to issue free shares of common stock to registered website users, as part of a broader promotion to attract traffic to the website and promote brand awareness and loyalty. The SEC took the view that the free distribution of shares was a "sale" of securities.⁷⁸ Similarly, the SEC has taken the view that the spin-off of shares of a subsidiary as a free stock dividend to an issuer's shareholders can be a sale of securities.⁷⁹ As a result, unless and until the SEC gives more lenient guidance, airdrops should be considered and conducted in the same manner as token offerings, generally, as discussed above.

Although sufficient decentralization is difficult to define precisely, there are potential steps that the SEC can take to provide market participants with greater clarity. The SEC has highlighted a number of factors to consider when inquiring whether a token-based network is sufficiently decentralized. Of course, as noted by Commissioner Peirce,⁸⁰ it would be helpful if the SEC could provide clarity as to the appropriate weighting of such factors. One of the primary goals of securities law is to protect investors through the mitigation of information asymmetries that exist between issuers and investors. We propose that this principle should inform the weighting of the factors used to measure the sufficient decentralization of a network. As a result, there should be less emphasis on factors that penalize tokens simply because they bear similarity to securities in their marketing, and greater emphasis on factors that have a clear nexus to the reduction of information asymmetries. For example, the decentralization of network development and maintenance as well as network governance should be factors that are amongst the most heavily weighted. If such activity is truly decentralized, the less likely it is for there to be information asymmetries between network users and a powerful central group that manages the network.

On the other hand, the SEC should give less weight to factors such as a token's transferability or the existence of secondary markets for it. As discussed, a commodity does not become a security simply because there are secondary markets on which it is traded. It is critical to the success of certain token-based networks to have a large number of active market participants. If users on such networks were restricted from exchanging in some way their tokens with other potential participants, it is unlikely that the network could reach the necessary critical mass.

Furthermore, the SEC should provide clear guidance regarding potential pathways for achieving sufficient decentralization. Under the current regulatory framework, developers need to be wary that the seeding of their network via token "airdrops" and other distributions to affiliates, strategic partners, vendors and community members could be deemed to be a securities offering given that the issuer may receive a direct benefit from such distributions. However, these parties are unlikely to require protection from the information asymmetries securities laws are designed to guard against and these distributions are a vital step for many networks to be able to achieve decentralization. Such distributions often promote network activity, facilitate the implementation of governance procedures, enable network testing prior to full launch and incentivize third-party development work. In addition, this seed activity permits the nascent token economy of a network to grow, allowing forces beyond those of the initial promoter to begin to determine the network's value. As a result, this activity directly addresses several of the factors identified in the Framework and can strengthen the case that a particular network is decentralized.

Conclusion

Much has been made of the need for certainty, and perhaps even innovation, in the application of various laws, including the US securities and commodities laws, to commercial activities relating to blockchain, cryptocurrencies and related technologies. After all, the applicable federal securities statute is over 85 years old, and the seminal case, *Howey*, is more than 70 years old. That said, the SEC has not retreated from the application of existing precedent when examining token transactions. Nevertheless, given the underlying principles, and the SEC's public statements, there is some reason for optimism that the existing framework will permit at least some transactions in tokens – consumer token launches – to be executed without the application of the federal securities laws. We suggest, however, that it continues to be prudent for interested parties to seek guidance directly from the SEC staff before proceeding.

Endnotes

1. Robert Stevens, *SEC Faces Stiff Test in Regulating DeFi, Says Hester Peirce*, Decrypt (Sept. 4, 2020), <https://decrypt.co/40819/sec-faces-stiff-test-regulating-defi-says-hest-er-peirce>.
2. Jack Purdy, *DEXs Threaten Centralized Exchange Dominance as Share of Total Volumes Exceed 5%*, Messari (Sept. 3, 2020), <https://messari.io/article/dexs-threaten-centralized-exchange-dominance-as-share-of-total-volumes-exceed-5>.
3. *Nifty Gateway Sets New Record for Digital Art Sale*, Gemini (Aug. 5, 2020), <https://gemini.com/blog/nifty-gateway-sets-new-record-for-digital-art-sale>.
4. Mason Nystrom, *WHALE Token and the Rise of Nonfungible Liquidity Mining*, Messari (Sept. 9, 2020), <https://messari.io/article/whale-token-and-the-rise-of-nonfungible-liq-uidity-mining>.
5. The Digital Asset Taxonomy published by ConsenSys, a leader in the blockchain field, defined “consumer tokens” as “inherently consumptive in nature, which means that their intrinsic features and primary use are to represent, or facilitate the exchange of or access to, a limited set of goods, services, or content. The term “consumer” here refers to the consumptive nature of the relevant goods, services, or content, which businesses as well as individual users may ultimately use or consume[.]” DIGITAL ASSET TAXONOMY: FROM THE PERSPECTIVE OF GLOBAL FRAMEWORKS FOR SECURITIES AND FINANCIAL INSTRUMENTS, <https://thebcp.com/token-taxonomy/> (last visited July 26, 2018).
6. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
7. 15 U.S.C. §§ 77b(a)(1), 78c(a)(10).
8. *See Howey* at 301.
9. *See id.*
10. *See* Latham & Watkins, SEC Takes Enforcement Action against Utility Token ICO, Client Alert No. 2257 (Dec. 20, 2017), <https://www.lw.com/thoughtLeadership/SEC-vigorously-police-utility-token-ICO>.
11. *Gary Plastic Packaging v. Merrill Lynch, Pierce, Fenner, & Smith Inc.*, 756 F.2d 230 (2d Cir. 1985).
12. Hester M. Peirce, *Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization* (Feb. 6, 2020), <https://www.sec.gov/news/speech/peirce-remarks-blockress-2020-02-06>.
13. SEC, *Framework for “Investment Contract” Analysis of Digital Assets* (2019), <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>.
14. TurnKey Jet, Inc., SEC No-Action Letter (Apr. 3, 2019), <https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm>; Pocketful of Quarters, Inc., SEC No-Action Letter (July 25, 2019), <https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1>.
15. *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019).
16. *Id.*
17. *Kik Responds to SEC Complaint*, PR Newswire (June 4, 2019), <https://www.prnewswire.com/news-releases/kik-responds-to-sec-complaint-300862114.html> [hereinafter *Kik Response Article*].
18. Wells Submission of Kik Interactive Inc. and the Kin Ecosystem Foundation at 17 (Dec. 10, 2018), https://www.kin.org/wells_response.pdf.
19. *Kik Response Article*.
20. *Telegram to Return \$1.2 Billion to Investors and Pay \$18.5 Million Penalty to Settle SEC Charges*, Sec. & Exch. Comm’n (June 26, 2020), <https://www.sec.gov/news/press->

- release/2020-146; *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) (S.D.N.Y. filed Mar. 20, 2020).
21. *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019); *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) (S.D.N.Y. filed Mar. 20, 2020).
 22. *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) at 2 (S.D.N.Y. filed Mar. 20, 2020).
 23. *See, e.g.*, 7 U.S.C. §§ 6c(a), 9, 12(a)(5), 15; 17 C.F.R. § 180.1; *see also* Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41398 (July 14, 2011), <https://www.gpo.gov/fdsys/pkg/FR-2011-07-14/pdf/2011-17549.pdf>.
 24. Timothy Massad, Chairman, Commodity Futures Trading Comm'n, Testimony of Chairman Timothy Massad before the US Senate Committee on Agriculture, Nutrition & Forestry (Dec. 10, 2014), <http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6> [hereinafter 2014 Massad Senate Testimony].
 25. During this time, the CFTC has settled enforcement actions with exchanges, stressing a distinct aspect of its jurisdictional oversight in each: from establishing that virtual currencies are “commodities,” to applying the retail commodity rules to leveraged virtual currency transactions, to asserting jurisdiction over virtual currency derivatives. *See* Latham & Watkins, CFTC Brings Significant Enforcement Action Against Online Cryptocurrency Exchange, Client Alert No. 1980 (June 20, 2016), <https://www.lw.com/thoughtLeadership/CFTC-brings-significant-enforcement-action-against-online-cryptocurrency-exchange>; Latham & Watkins, Enforcement Trends in Cryptocurrency, Client Alert No. 1904 (Dec. 9, 2015), <https://www.lw.com/thoughtLeadership/lw-enforcement-trends-cryptocurrency>; Latham & Watkins, Cryptocurrencies Are Commodities: CFTC’s First Bitcoin Enforcement Action, Client Alert No. 1874 (Sept. 21, 2015), <https://www.lw.com/thoughtLeadership/LW-CFTC-first-bitcoin-enforcement-action>.
 26. *See, e.g.*, CFTC Release PR7938-19, CFTC Charges Company and its Principal in \$147 Million Fraudulent Bitcoin Trading Scheme (June 18, 2019), <https://www.cftc.gov/PressRoom/PressReleases/7938-19>; CFTC Release PR7839-18, CFTC Orders Former Virtual Currency Trader to Pay More than \$1.1 Million for Fraudulent Bitcoin and Litecoin Scheme (Nov. 9, 2018), <https://www.cftc.gov/PressRoom/PressReleases/7839-18>; CFTC Release PR7813-18, CFTC Charges Two Defendants with Fraudulent Solicitation, Impersonation of a CFTC Investigator, and Forging CFTC Documents, All in Attempt to Steal Bitcoin (Sept. 28, 2018), <https://www.cftc.gov/PressRoom/PressReleases/7813-18>; CFTC Release PR7714-18, CFTC Charges Multiple Individuals and Companies with Operating a Fraudulent Scheme Involving Binary Options and a Virtual Currency Known as ATM Coin (April 18, 2018), <https://www.cftc.gov/PressRoom/PressReleases/7714-18>; CFTC Release PR7614-17, CFTC Charges Nicholas Gelfman and Gelfman Blueprint, Inc. with Fraudulent Solicitation, Misappropriation, and Issuing False Account Statements in Bitcoin Ponzi Scheme (Sept. 21, 2017), <http://www.cftc.gov/PressRoom/PressReleases/pr7614-17>.
 27. The following discussion of consumer token presales only seeks to address fundraising instruments utilized for pure consumer token issuances and not instruments utilized for pure security token issuances, which often have similar terms. We note that the presale of a token designed to be a security is a far easier analysis, as each of the instruments should be offered and sold in compliance with securities law requirements and ordinary corporate finance practices.
 28. *See, e.g.*, Juan Batiz-Benet, Jesse Clayburgh & Marco Santori, THE SAFT PROJECT: TOWARD A COMPLIANT TOKEN SALE FRAMEWORK (Oct. 2, 2017), <https://saftproject.com/static/SAFT-Project-Whitepaper.pdf> [hereinafter SAFT Whitepaper].

29. In addition to the securities law issues and commodities law issues discussed below, the SAFT and similar presale instruments can raise tax concerns in light of the uncertainty regarding their treatment for US federal income tax purposes. It is possible that an issuer could be subject to US federal income tax on proceeds from SAFT sales on a current basis, particularly where the underlying tokens are consumer tokens.
30. *Id.* (Section 5(c) of the SAFT, which is included as Exhibit 1 to the SAFT Whitepaper): “(c) The Purchaser has no intent to use or consume any or all Tokens on the corresponding blockchain network for the Tokens after Network Launch. The Purchaser enters into this security instrument purely to realise profits that accrue from purchasing Tokens at the Discount Price.”
31. Defined in the SAFT as “a *bona fide* transaction or series of transactions, pursuant to which the [issuer] will sell the Tokens to the general public in a publicized product launch.” Simple Agreement for Future Tokens, <https://saftproject.com/static/Form-of-SAFT-for-token-pre-sale.docx> (last visited July 29, 2018).
32. We note that some practitioners have proposed that if the network launch occurs more than six months after the SAFT sale, they should constitute two distinct plans of financing and thus would not be integrated in accordance with the safe harbor of Rule 502 under the Securities Act. In this regard, we would consider the concurrent settlement to negate this proposition. Similarly, the SAFT itself may constitute an offering of the underlying token that is continuous until delivery. In any event, we would expect that the tokens received by SAFT investors would nevertheless constitute securities on the date of delivery given the nature of the SAFT offering and the delivery of tokens to investors, unless the network has become sufficiently decentralized in the interim such that the “efforts” prong of the *Howey* Test was no longer satisfied.
33. It is worth noting, however, that the US House of Representatives recently passed several bills aimed at improving capital formation for smaller companies. For example, the Main Street Growth Act would amend the Securities Exchange Act of 1934, as amended, to allow registration of venture exchanges that would provide trading venues tailored for smaller companies, such as blockchain-based start-ups, whose securities are considered less liquid than those of larger companies. Main Street Growth Act, H.R. 5877, 115th Congress (as passed by House, July 10, 2018), <https://www.congress.gov/bill/115th-congress/house-bill/5877>; see Tom Zanki, *House Passes Bill to Allow Venture Exchanges*, LAW360 (July 11, 2018), <https://www.law360.com/articles/1062096/house-passes-bill-to-allow-venture-exchanges>.
34. See 15 U.S.C. § 78c(a)(4)(A) (defining “broker” as “any person engaged in the business of effecting transactions in securities for the account of others”); 15 U.S.C. § 78c(a)(5)(A) (defining “dealer” as “any person engaged in the business of buying and selling securities . . . for such person’s own account”); 15 U.S.C. § 78c(a)(1) (defining “exchange” as “any organization, association or group of persons, whether incorporated or unincorporated, which constitutes, maintains or provides a marketplace or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange as that term is generally understood, and includes the market place and the market facilities maintained by such exchange”).
35. See William Hinman, Dir., Div. Corp. Fin., Sec. & Exch. Comm’n, *Digital Asset Transactions: When Howey Met Gary (Plastic)* (June 14, 2018), <https://www.sec.gov/news/speech/speech-hinman-061418> [hereinafter Hinman Speech].
36. See *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019).; *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) (S.D.N.Y. filed Mar. 20, 2020).

37. *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019).
38. *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) at 43 (S.D.N.Y. filed Mar. 20, 2020).
39. *See, e.g.*, 2014 Massad Senate Testimony.
40. *See* 7 U.S.C. § 1a(47)(A)(ii) (“the term ‘swap’ means any agreement, contract, or transaction . . . that provides for any purchase, sale, payment, or delivery . . . that is dependent on the occurrence, nonoccurrence, or the extent of the occurrence of an event or contingency associated with a potential financial, economic, or commercial consequence”). Swap contracts are subject to a myriad of CFTC regulations under the CEA, as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the Dodd-Frank Act), including the requirement that over-the-counter (OTC) swap counterparties be “eligible contract participants.” *Id.* § 1a(18) (defining eligible contract participants (ECPs)). An individual can only qualify as an ECP if such person has amounts invested on a discretionary basis, the aggregate of which is in excess of \$10 million; or \$5 million and enters into swaps in order to manage the risk associated with an asset owned or liability incurred (or reasonably likely to be owned or incurred) by such person. *Id.* § 1a(18)(A) (xi). If one or both of the parties to a swap transaction are non-ECPs, the swap must be executed on a CFTC-registered designated contract market. *Id.* § 2(e).
41. Both the CEA and CFTC regulations thereunder have long recognized a forward contract exclusion from futures contracts. *See* 7 U.S.C. § 1a(27) (“The term ‘future delivery’ does not include any sale of any cash commodity for deferred shipment or delivery.”). Following enactment of the Dodd-Frank Act in 2010, the sale of a non-financial commodity for deferred shipment or delivery was also excluded from the definition of “swap” in Section 1a(47) of the CEA under the Non-Financial Forward Contract Exclusion. *Id.* § 1a(47)(B)(ii).
42. 17 C.F.R. § 34.3(a).
43. Both the CEA and CFTC regulations thereunder have long recognized a forward contract exclusion from futures contracts. *See* 7 U.S.C. § 1a(27) (“The term ‘future delivery’ does not include any sale of any cash commodity for deferred shipment or delivery.”). Following enactment of the Dodd-Frank Act in 2010, the sale of a non-financial commodity for deferred shipment or delivery was also excluded from the definition of “swap” in Section 1a(47) of the CEA under the Non-Financial Forward Contract Exclusion. *Id.* § 1a(47)(B)(ii).
44. *See* Further Definition of “Swap,” “Security-Based Swap,” and “Security-Based Swap Agreement;” Mixed Swaps; Security-Based Swap Agreement Recordkeeping, 77 Fed. Reg. 48208, 48228 (Aug. 13, 2012), <https://www.gpo.gov/fdsys/pkg/FR-2012-08-13/pdf/2012-18003.pdf> [hereinafter *Products Release*].
45. As the CFTC has noted, “the underlying postulate of the [forward] exclusion is that the [CEA’s] regulatory scheme for futures trading simply should not apply to private commercial merchandising transactions which create enforceable obligations to deliver but in which delivery is deferred for reasons of commercial convenience or necessity.” *Id.* at 48228.
46. The CFTC drew a clear distinction between commercial market participants and investors in the *Products Release*, stating that “[a] hedge fund’s investment activity is not commercial activity within the CFTC’s longstanding view of the Brent Interpretation.” *Id.* at 48229. The “Brent Interpretation” refers to the CFTC’s 1990 interpretation of the application of the forward contract exclusion from the definition of “future delivery” in the context of “book-outs” transactions, which the CFTC extended in the *Products Release* to apply to the forward contract exclusion from the swap definition for non-financial commodities.

Statutory Interpretation Concerning Forward Transactions, 55 Fed. Reg. 39188 (Sept. 25, 1990), <https://cdn.loc.gov/service/ll/fedreg/fr055/fr055186/fr055186.pdf>.

Moreover, the CFTC continued to elaborate on its discerning view of “commercial” in the Products Release, stating that “an investment vehicle taking delivery of gold as part of its investment strategy would not be engaging in a commercial activity within the meaning of the Brent Interpretation.” Products Release at 48229. However, if the investment vehicle were to own a chain of jewelry stores and would purchase gold on a forward basis to provide raw materials for the jewelry store, the CFTC would consider such activity to fall within the forward contract exclusion under the Brent Interpretation. *Id.* Notably, the CFTC stated in the Products Release that, for purposes of the “swap” definition, the Non-Financial Forward Contract Exclusion will be interpreted in a manner consistent with the CFTC’s historical interpretation of the existing forward exclusion with respect to futures. As a result, the Brent Interpretation analysis is applicable for purposes of evaluating the Non-Financial Forward Contract Exclusion as it pertains to the “swap” definition. *Id.* at 48227–48228.

47. *See id.*; *supra* text accompanying note 20.
48. 7 U.S.C. § 1a(47)(A)(i) (“the term ‘swap’ means any agreement, contract, or transaction . . . that is a put, call, cap, floor, collar, or similar option of any kind that is for the purchase or sale, or based on the value, of 1 or more . . . commodities”).
49. *See* 17 C.F.R. § 32.3(c).
50. *See* 17 C.F.R. § 32.3(a).
51. Under Section 2(f) of the CEA, a hybrid instrument is “predominantly a security” and exempt from the provisions of the CEA if:
 1. the hybrid instrument issuer receives payment in full of the hybrid instrument’s purchase price, substantially contemporaneously with delivery of the hybrid instrument;
 2. the hybrid instrument purchaser/holder is not required to make any payment to the issuer in addition to the purchase price described above, whether as margin, settlement payment or otherwise, during the life of the hybrid instrument or at maturity;
 3. the hybrid instrument issuer is not subject by the instrument’s terms to mark-to-market margining requirements; and
 4. the hybrid instrument is not marketed as a contract of sale of a commodity for future delivery (or option on such a contract) subject to the CEA.
 7 U.S.C. § 2(f)(2).
52. This discussion assumes that prongs (i)–(iii) of the Hybrid Instrument Exemption are met with respect to any such presale instrument. Any such presale instrument must meet all four prongs of the exemption.
53. *See supra* text accompanying note 27; 7 U.S.C. § 2(e).
54. Such securities offerings are almost exclusively accomplished through the use of an exemption from registration, such as in a private placement that is limited to participants who are “accredited investors,” as defined in 17 C.F.R. § 230.501, either under the more traditional-style private placement of Regulation D, Rule 506(b), or the crowdfunding compatible, Regulation D, Rule 506(c). Issuers may also consider utilizing Regulation CF or Regulation A, which permit sales to non-accredited investors after making certain filings with the SEC. For additional information, *see* Latham & Watkins, SEC Adopts Final Crowdfunding Rules, Client Alert No. 1893 (Nov. 10, 2015), <https://www.lw.com/thoughtLeadership/lw-sec-adopts-crowdfunding-rules>; Stephen P. Wink and Brett M. Ackerman, Crowdfunding Under the SEC’s New Rules, 49 REV. OF SEC. &

- COMMODITIES REG. 267 (Dec. 21, 2016), <https://www.lw.com/thoughtLeadership/crowdfunding-SEC-new-rules-2016>.
55. While issuers should be cautious when granting such rights, generally the enterprise and its investors are best served when their interests align. In consumer token sales, the parties share a direct interest in ensuring the offering or distribution complies with applicable securities and commodities laws. In addition, all participants should share a similar interest in the maturing of the market for token presales, as in the traditional venture capital space, to attract capital from investors that have yet to approach the sector due to regulatory risks.
 56. A discussion of the types of structures that may so qualify and the nature of the availability of the possible exemptions is beyond the scope of this chapter.
 57. See Latham & Watkins, *Token Presale Agreements and the ConsenSys Automated Convertible Note* (May 22, 2019), <https://www.lw.com/thoughtLeadership/token-presale-agreements-consensys-automated-convertible-note>.
 58. See Hinman Speech; see also Latham & Watkins, *A Path Forward for Consumer Tokens*, Client Alert No. 2336 (June 27, 2018), <https://www.lw.com/thoughtLeadership/lw-a-path-forward-for-consumer-tokens>.
 59. See Hinman Speech.
 60. *SEC v. Glenn W. Turner Enterprises Inc.*, 474 F.2d 476, 482 (9th Cir. 1973) (“[T]he fact that the investors here were required to exert some efforts if a return were to be achieved should not automatically preclude a finding that the Plan or Adventure is an investment contract. To do so would not serve the purpose of the legislation. Rather we adopt a more realistic test, whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise.”); see *United Housing Found., Inc. v. Forman*, 421 U.S. 837, 855 (1975) (the “efforts of others” prong of the *Howey* Test requires that investors have a reasonable expectation of profit derived from the efforts of others).
 61. In *Noa v. Key Futures, Inc.*, the Ninth Circuit held that if the expectation of economic return from an instrument is based solely on market forces, and not on the efforts of a promoter, then the instrument does not satisfy this prong of the *Howey* Test. *Noa v. Key Futures, Inc.*, 638 F.2d. 77 (9th Cir. 1980). The scheme in *Noa* involved the sale of silver bars through high-pressure sales efforts, and the Ninth Circuit’s decision rested primarily on the existence of a separate market for the instrument that the investor could sell into, such that the economic return was driven by the market price and not the efforts of the promoter: “Once the purchase of silver bars was made, the profits to the investor depended upon the fluctuations of the silver market, not the managerial efforts of Key Futures. The decision to buy or sell was made by the owner of the silver.” *Id.* at 79. *SEC v. Belmont Reid & Co.* involved a promoter that was involved in a gold mining operation who obtained prepayments from investors for the purchase of gold coins that would be obtained as a result of the mining operation. *SEC v. Belmont Reid & Co.*, 794 F.2d 1388 (9th Cir. 1986). While the purchaser’s return was highly dependent on the ability of the promoter to successfully mine and deliver the gold coins, the Ninth Circuit reasoned that the same non-performance risk exists in the context of any sale-of-goods contract in which the buyer pays in advance, and therefore that such a dependence on the promoter’s efforts could not itself satisfy the *Howey* Test without making any such sale-of-goods contract a security. Instead, the Ninth Circuit held that the *Howey* Test was not satisfied in *Belmont Reid & Co.*, because the purchasers who prepaid for the gold coins: “[H]ad as their primary purpose to profit from the anticipated increase in

the world price of gold . . . In short, the purchaser[s] were speculating in the world gold market . . . To the extent the purchasers relied on the managerial skill of [the promoters] they did so as an ordinary buyer, having advanced the purchase price, relies on an ordinary seller.” *Id.* at 1391.

62. *See id.*
63. *See supra* text accompanying note 47.
64. Please note that we have chosen Filecoin in this example in part because we have no connection to its activities.
65. Protocol Labs, FILECOIN: A DECENTRALIZED STORAGE NETWORK (Aug. 14, 2017), <https://filecoin.io/filecoin.pdf>.
66. CoinList, FILECOIN TOKEN SALE ECONOMICS, https://coinlist.co/assets/index/filecoin_index/Filecoin-Sale-Economics-e3f703f8cd5f644aec7ae3860ce932064ce014dd60de115d67ff1e9047ffa8e.pdf (last visited July 26, 2018).
67. Hinman Speech; *see Munchee* Order; Jay Clayton, Chairman, Sec. & Exch. Comm’n, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>.
68. Hinman Speech.
69. Jay Clayton, Chairman, Sec. & Exch. Comm’n, Chairman’s Testimony on Virtual Currencies: The Roles of the SEC and CFTC, (Feb. 6, 2018), <https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission>. (“In short, prospective purchasers are being sold on the potential for tokens to increase in value with the ability to lock in those increases by reselling the tokens on a secondary market or to otherwise profit from the tokens based on the efforts of others. These are key hallmarks of a security and a securities offering.”)
70. *See Gary Plastic* at 240–241.
71. *See* Hinman Speech (“Are the tokens distributed in ways to meet users’ needs? For example, can the tokens be held or transferred only in amounts that correspond to a purchaser’s expected use? Are there built-in incentives that compel using the tokens promptly on the network, such as having the tokens degrade in value over time, or can the tokens be held for extended periods for investment?”).
72. *See id.* (“Is token creation commensurate with meeting the needs of users or, rather, with feeding speculation?”).
73. *See id.* (“Has this person or group retained a stake or other interest in the digital asset such that it would be motivated to expend efforts to cause an increase in value in the digital asset?”).
74. *Id.*
75. Pocketful of Quarters, Inc., SEC No-Action Letter (July 25, 2019), <https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1>.
76. *See* Hinman Speech (“Are independent actors setting the price or is the promoter supporting the secondary market for the asset or otherwise influencing trading?”).
77. *See id.* (“Are the assets dispersed across a diverse user base or concentrated in the hands of a few that can exert influence over the application?”).
78. Simplystocks.com, SEC No-Action Letter (Feb 4, 1999).
79. SEC Staff Legal Bulletin No. 4 (Sept. 16, 1997), <https://www.sec.gov/interp/legalslbcf4.txt>.
80. Hester M. Peirce, How We Howey (May 9, 2019), <https://www.sec.gov/news/speech/peirce-how-we-howey-050919>.

Acknowledgments

In addition to the co-authors listed below, the authors gratefully acknowledge the invaluable contributions of Shaun Musuka and J. Ashley Weeks.

Paul M. Dudek

Tel: +1 202 637 2377 / Email: paul.dudek@lw.com

Paul Dudek is a partner in the Washington, D.C. office of Latham & Watkins. From 1993 to 2016, he was Chief of the Office of International Corporate Finance in the US Securities Exchange Commission's (SEC) Division of Corporation Finance. Mr. Dudek has deep experience in SEC registrations, and his practice covers all aspects of cross-border capital market transactions involving non-US companies and sovereigns, as well as related regulatory matters. In his previous role, Mr. Dudek oversaw the Office's efforts to develop and implement rulemaking initiatives and interpretive policies pertaining to US public and private offerings, listings and other transactions and periodic reporting by foreign private issuers in the US and multinational offerings by foreign and domestic issuers.

Miles P. Jennings

Tel: +1 650 463 3063 / Email: miles.jennings@lw.com

Miles Jennings is a partner in the San Francisco and Silicon Valley offices of Latham & Watkins. Mr. Jennings represents public and private technology, life science, cryptocurrency and other growth companies, as well as the entities that finance them. His practice focuses on general corporate counseling, venture capital financings, cryptocurrency offerings, mergers and acquisitions, and public offerings. Mr. Jennings' general company representation includes assistance with formation issues, employment matters, equity incentives, securities law compliance, negotiation of license agreements, and advising boards of directors regarding corporate governance matters.

**David L. Concannon****Tel: +1 212 906 1389 / Email: david.concannon@lw.com**

David Concannon is a partner in the New York office of Latham & Watkins where he is a member of the firm's Emerging Companies Practice. Mr. Concannon is among a select few lawyers in New York whose practices focus exclusively on emerging companies, representing both clients as company counsel and venture capital firms as investor counsel. He advises emerging companies through their entire lifecycle, from formation through growth stages and exits. Mr. Concannon spends substantial time advising market participants regarding cryptocurrencies and initial coin offerings, and serves as a Co-Chair of the firm's Blockchain and Cryptocurrency Task Force.

**Yvette D. Valdez****Tel: +1 212 906 1797 / Email: yvette.valdez@lw.com**

Yvette Valdez is a partner in the New York office of Latham & Watkins and a member of the Derivatives Practice, Financial Institutions Group, and FinTech Industry Group. Ms. Valdez advises emerging companies, financial institutions, and investment managers on complex regulatory challenges in the development of bespoke financial crypto-asset and cryptocurrency technologies, including token sales, market infrastructure, trading, clearing, and settlement solutions on distributed ledger technology. She also advises clients on domestic and cross-border fintech initiatives in the derivatives markets. Ms. Valdez also has significant experience representing dealers, intermediaries, and end-users in connection with derivatives (swaps and futures) legal and regulatory matters under the Dodd-Frank Act, the Commodity Exchange Act, as well as related CFTC, SEC, and prudential regulation.

**Stephen P. Wink****Tel: +1 212 906 1229 / Email: stephen.wink@lw.com**

Stephen Wink is a partner in the New York office of Latham & Watkins and a member of the Financial Institutions Group and FinTech Industry Group. Mr. Wink is Co-Chair of the firm's Blockchain and Cryptocurrency Task Force. His practice focuses on advising a wide range of market players, including fintech companies, cryptocurrency issuers and platforms, investment banks, hedge funds, private equity firms, trading platforms, and other financial institutions. Mr. Wink has in-depth knowledge and broad experience advising institutions on regulatory and related matters, gained in part from a decade as general counsel of a full-service investment bank.

Latham & Watkins LLP

885 Third Avenue, New York, New York 10022, USA
Tel: +1 212 906 1200 / Fax: +1 212 751 4864 / URL: www.lw.com

An introduction to virtual currency money transmission regulation

Michelle Ann Gitlitz, Carlton Greene & Caroline Brown
Crowell & Moring LLP

Introduction

Virtual currencies allow individuals to effectuate fast, low-cost, seamless, and secure cross-border transactions. For regulators, the proliferation of virtual currencies and these transactions has also increased potential money laundering, terrorism finance, and consumer protection concerns. This chapter examines when businesses in the virtual currency arena may be obligated to comply with federal and state money transmission laws and regulations in the United States.

At the federal level, the Bank Secrecy Act (“BSA”)¹ requires banks, broker-dealers, money services businesses (“MSBs”), and many other types of financial institution to file certain reports, including in particular suspicious activity reports (“SARs”), to maintain certain records, and to maintain anti-money laundering (“AML”) programs designed to prevent the institution from being used to facilitate financial crime. The Financial Crimes Enforcement Network (“FinCEN”), a bureau of the U.S. Department of the Treasury, administers the BSA and is charged with protecting the U.S. financial system and combating money laundering and terrorism financing. FinCEN does this through the civil enforcement of BSA rules against regulated financial institutions, the promulgation of additional AML rules and guidance, and by maintaining a database of the reporting it receives from regulated financial institutions and other law enforcement information. FinCEN makes this information available to federal, state, and local law enforcement agencies as well as financial regulators to aid their law enforcement missions. In addition, FinCEN produces its own analysis of the data to identify money laundering, terrorism financing, and other threats to the financial system and to make referrals to law enforcement. FinCEN is also the U.S. Financial Intelligence Unit (“FIU”), and cooperates with a network of more than 140 foreign FIUs to share information on such threats.² Many virtual currency businesses are regulated under the BSA as money transmitters, a form of MSB.

Separate from the federal regulations, nearly every U.S. state has its own laws governing money transmitters. There is some overlap in the design of these laws, but also many differences, requiring individualized consideration of each state. In many cases, these laws are vaguely drafted, or were designed in an era that did not contemplate virtual currency. Unlike federal AML rules, state money transmission laws often are not aimed at protecting against money laundering and terrorist financing; rather, they focus on consumer protection, ensuring that a money transmitter will not lose, steal, or misdirect the consumer’s money.

The obligation of virtual currency businesses to consider not only federal law, but also a patchwork of varying state money transmitter statutes, has proven to be one of greatest regulatory challenges that virtual currency businesses face. The maze of state licensing

regulations paired with FinCEN's federal requirements demand thoughtful consideration of legal compliance for any person or business that operates in the virtual currency industry.

Federal virtual currency money transmission

The BSA is a composite of multiple statutes starting with the Currency and Financial Transactions Reporting Act of 1970, as amended by Title III of the USA PATRIOT Act of 2001 and other legislation.³

The BSA requires "financial institutions" to monitor their customers and their transactions and to identify and report suspicious activity to FinCEN in the form of SARs.⁴ Financial institutions that encounter certain "red flags" of potential money laundering or terrorism financing associated with a customer or transaction are expected to investigate these indicators to determine whether a legitimate explanation for the activity can be found. If not, the institutions must file a SAR.⁵ Periodically, FinCEN also publishes advisories and alerts providing additional red flags relating to specific industries or types of illicit activities. As an example, in July 2020, FinCEN published an alert providing red flags relating to a virtual currency scam involving the social media service, Twitter, and asked convertible virtual currency ("CVC") exchanges and other financial institutions to report similar suspicious transactions to FinCEN.

In addition to filing SARs and other reports with FinCEN, banks and broker-dealers are required to conduct customer due diligence ("CDD") to understand the nature and purpose of their customers' relationships with the institution and to operate customer identification programs ("CIPs"), under which they must obtain and verify certain identifying information about their customers, such as full name, date of birth, address, and a taxpayer identification number such as a Social Security number.⁶ Money transmitters, as a form of MSB, are subject to slightly different requirements: they do not have a categorical obligation to identify all customers, but must do so when they send or receive transactions of \$3,000 or more for a customer. However, they must register with FinCEN,⁷ and renew this registration periodically thereafter. As noted above, to the extent that virtual currency businesses become subject to the BSA, it usually is because they qualify as a "money transmitter," and therefore as an MSB.

Whether an entity or individual qualifies as a "money transmitter" is determined by the type of activities in which that person or entity engages. A money transmitter is a person "wherever located" that engages as a business "wholly or in substantial part in the United States" in the provision of money transmission⁸ services. "Money transmission services" are defined to include "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."⁹ "Any means" includes "through a financial agency or institution," such as the use of a bank account. This concept is very broad, both in the breadth of transactions potentially covered, and in the fact that it includes foreign entities that provide money transmission services to persons in the U.S.¹⁰

FinCEN Virtual Currency Guidance

Although the rules governing money transmitters were not established specifically with virtual currency in mind, they are drafted broadly and were intended to be adaptable to a wide variety of conduct. FinCEN has sought to fill in gaps in their interpretation within the specific context of virtual currencies by providing guidance on this issue, in particular two substantial pieces of guidance in March 2013 and May 2019.

In its 2013 Guidance, FinCEN explained that it defines “value that substitutes for currency” under the money transmission standard to include “convertible virtual currency.”¹¹ The Guidance defines “virtual currency” as “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency.”¹² A “convertible” virtual currency is one that “has an equivalent value in real currency, or acts as a substitute for real currency.”¹³ Perhaps most importantly, FinCEN treats the exchange of fiat currency for virtual currency as the transmission of “currency, or value that substitutes for currency” from one location – the purchaser’s fiat wallet – to another, i.e., to a new virtual currency wallet, and therefore as “money transmission.”¹⁴ The Guidance also identifies three categories of participants in the virtual currency ecosystem: users; exchangers; and administrators, described below.¹⁵

- **User:** A person who “obtains virtual currency to purchase goods or services” is a user.¹⁶ This includes businesses that are strictly investing in CVC for their own account and not for any other party.¹⁷ Under the current Guidance, institutions investing in virtual currencies, such as co-mingled investment funds, are likely considered users. The method of obtaining virtual currency (e.g., “earning,” “harvesting,” “mining,” “creating,” “auto-generating,” “manufacturing,” or “purchasing”) is not determinative of whether a person qualifies as a “user,” an “administrator” or an “exchanger.”¹⁸
- **Exchanger:** “A person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency” is an exchanger.¹⁹ Importantly, a person must be engaged as a business; thus, trading simply for personal investment purposes does not qualify one as an exchanger. In addition, one must accept and transmit virtual currency from one person to another or to another location. This covers transactions where the parties are exchanging fiat and CVC, and transactions where parties are exchanging one virtual currency for another virtual currency. However, the mere acceptance of virtual currency in exchange for providing a good or service does not make a person a money transmitter.
- **Administrator:** A person engaged as a business in issuing (i.e., putting into circulation) a virtual currency, and who has the authority to redeem (i.e., to withdraw from circulation) such virtual currency, is an administrator.²⁰

Users are not considered money transmitters, and thus are not required to register with FinCEN or otherwise comply with BSA regulations. Exchangers or administrators may be considered money transmitters and may be required to register with FinCEN and comply with BSA regulations, depending on the specific facts and circumstances of the entity’s business model.

Classification of persons and entities conducting virtual currency business activities for money transmission purposes

Since issuing the Guidance in March 2013, FinCEN has issued subsequent Guidance on virtual currency that further informs the application of existing money transmission regulations to various business models in the virtual currency arena, including the following:

Guidance

- *Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019); and
- *Advisory on Illicit Activity Involving Convertible Virtual Currency*, FIN-2019-A003 (May 9, 2019).

Administrative Ruling

- *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014) (the "2014 Software and Investment Ruling");
- *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001 (Jan. 30, 2014) (the "2014 Mining Ruling"); and
- *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System*, FIN-2014-R012 (Oct. 27, 2014) (the "2014 Payment System Ruling").

Below is a summary of how the FinCEN Guidance and the 2014 Payment System Ruling might apply to various players in the virtual currency market.

- **Anonymizing services:** Businesses providing anonymizing services (also known as "mixers" or "tumblers") that attempt to conceal the source of the transmission of virtual currency are money transmitters when they accept and transmit CVC and, therefore, have regulatory obligations under the BSA.²¹
- **Trading platforms and decentralized exchanges:** Peer-to-peer ("P2P") trading platforms are websites where CVC buyers and sellers can connect. Sometimes, these platforms also facilitate trades as an intermediary. Under FinCEN regulations, a person is exempt from money transmitter status if the person only provides the delivery, communication, or network access services used by a money transmitter to support money transmission services.²² Therefore, if a CVC trading platform only provides a forum where CVC buyers and sellers post their bids and offers (with or without automatic matching of counterparties), and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform), the trading platform may not qualify as a money transmitter under FinCEN regulations. By contrast, if a trading platform accepts CVC from a seller and then sells it to the buyer, the trading platform is acting as a CVC exchanger, and thus falls within the definition of money transmitter and its accompanying BSA obligations.²³
- **Software developer:** Whether software that facilitates the purchase or sale of virtual currency qualifies as money transmission for the developer depends on what the software does. Software that accomplishes the exchange of virtual currency between third parties is likely to be treated as money transmission by a developer or operator, but similar software that is used by a user to buy virtual currency for its own account may not be.²⁴
- **Miners:** Miners play a vital role in allowing many decentralized blockchain-based virtual currency systems to operate properly. Mining is important because virtual currencies or tokens, such as Bitcoin, are initially acquired through mining; unlike paper money, decentralized virtual currencies ("DVCs") do not have a central government to issue the currency. This provides a somewhat controlled way to distribute tokens and creates a real incentive for miners to enter the market. Miners also play another vital role: in the traditional banking system, banks maintain an accurate record of parties and details of each transaction; however, since there is no central regulator for DVCs, the miners assume this role.

Those who mine virtual currencies, whether by "earning," "harvesting," "creating," or "manufacturing," are classified as users and not money transmitters. Once the virtual currency is mined, a miner – depending on how he or she uses the CVC and for whose benefit – may potentially become a money transmitter.²⁵ Just because the miner acquired the tokens through mining, rather than purchasing or being given them, does not affect

his or her status as a user. Moreover, miners may use their mined tokens or currencies to purchase goods for their own use or investment. However, miners that mine tokens for the purposes of operating a business as an exchanger of CVC for fiat currency, or for other forms of CVC, are likely to be subject to regulation as an exchanger.

- **Centralized virtual currencies:** A virtual currency that has a centralized repository is a centralized virtual currency. The repository of a centralized virtual currency is a money transmitter to the extent that it allows transfers of value between persons or from one location (i.e., a user's account in New York) to another (i.e., that user's account in California). In addition, if the centralized virtual currency repository accepts currency or its equivalent from a user and privately credits the user with an appropriate portion of the repository's own CVC, and then transmits that internally credited value to third parties at the user's direction, the centralized virtual currency repository is a money transmitter.²⁶
- **Decentralized virtual currencies:** A DVC is a virtual currency that has no central repository and no single person who has the ability to issue or redeem the virtual currency. Persons may obtain the virtual currency through their own computing or mining effort or by purchasing the virtual currency. A person who creates units of a DVC and uses it to purchase real or virtual goods or services is a "user" of the CVC and is not subject to regulation as a money transmitter. By contrast, a person who creates units of a DVC, and sells those units to another person for real currency or its equivalent and is engaged in that exchange as a business, is a money transmitter.
- **Natural persons providing CVC money transmission (P2P exchangers):** FinCEN defines "money transmitter" to include both natural and legal persons engaged as a business in money transmission "whether or not on a regular basis or as an organized business concern."²⁷ P2P exchangers are generally natural persons engaged in the business of buying and selling CVCs. P2P exchangers facilitate transfers from one type of CVC to a different type of CVC, as well as exchanges between CVC and other types of value. P2P exchangers may provide their services online or in person. As the phrase quoted above suggests, a natural person operating as a P2P exchanger that engages in for-profit money transmission services involving real currency or CVCs is a money transmitter and must comply with BSA regulations, even if that person does not think of himself or herself as a "real" business. FinCEN recently took enforcement against an individual running such an exchange without registering as a money transmitter.²⁸ There is a narrow exemption for a natural person that engages in money transmission "on an infrequent basis and not for gain or profit," but for-profit activities fall outside of this.²⁹ As a money transmitter, P2P exchangers are required to comply with the BSA obligations that apply to money transmitters, including registering with FinCEN as an MSB and complying with the associated AML program, recordkeeping, and reporting requirements (including filing SARs and Currency Transaction Reports).³⁰
- **Wallets:** Wallets are virtual currency storage systems used to hold and potentially send or receive virtual currency. Most virtual currencies have official or suggested wallets and the use of a wallet is necessary. The wallet contains a public and private key for each virtual currency address. The private key is a secret number that allows the virtual currency to be spent. The public key is used to ensure that the wallet holder is the owner of the wallet address and can receive funds. The public key is mathematically derived from the private key. The status of a wallet provider as a money transmitter is affected by whether it has custody of the private keys for the virtual currency, which affects whether the wallet provider is deemed to have accepted and transmitted the funds sent using that key.

- **Custodial exchanges:** Custodial exchanges are virtual currency exchange platforms on which users are able to buy and sell virtual currencies. What distinguishes this type of exchange as custodial is the fact that the exchange is in control of a user's funds, or in other words, the exchange is the custodian of the private keys for the virtual currencies or tokens. Custodial exchanges typically are money transmitters because they are both buying and selling and accepting and transmitting virtual currencies.
- **Non-custodial "exchanges":** Companies that act merely as platforms to connect buyers and sellers of CVC but which do not accept funds from customers or hold or control private keys for customer CVC are less likely to qualify as money transmitters. Such services may act more akin to a message or classifieds board like Craigslist. Because they are never in possession of the currency or private keys, they are less likely to be considered to accept, transmit, buy, or sell virtual currencies.
- **Token issuers:** FinCEN has indicated that those who raise money through an initial coin offering ("ICO") by accepting fiat currency or other value in exchange for an immediate or subsequent distribution of CVC qualify as money transmitters.³¹ By contrast, an issuer that merely gives away, or "air drops," such tokens, may not be subject to regulation because it would not have exchanged tokens for another form of value.
- **Payment systems:** Virtual currency payment processing systems typically process payments and assist in executing transactions by accepting fiat from the buyer, keeping that fiat, and then paying the seller with the approximate market value of a virtual currency, or *vice versa*. By keeping a large reserve of virtual currency at all times, the payment processor is able to act as his or her own currency exchange to supply equivalent virtual currency in exchange for the fiat supplied by the buyer. According to FinCEN, payment processing systems that accept and convert both real and virtual currencies are money transmitters because they are exchangers and, therefore, must register.³² "An exchanger will be subject to the same obligations under FinCEN regulations regardless of whether it acts as a broker (attempting to match two (mostly) simultaneous and offsetting transactions involving the acceptance of one type of currency and the transmission of another) or as a dealer (transacting from its own reserve in either convertible virtual currency or real currency)."³³ There is, however, a carve-out from registration for payment processors when four conditions are met:
 - (i) the entity providing the service facilitates the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself);
 - (ii) the entity operates through clearance and settlement systems that admit only BSA-regulated financial institutions;
 - (iii) the entity provides the service pursuant to a formal agreement; and
 - (iv) the entity's agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds.³⁴
- **Bitcoin ATMs:** Generally, a fiat currency automated teller machine ("ATM") is not subject to FinCEN regulations as an MSB or money transmitter.³⁵ Fiat ATMs simply allow a consumer to access his or her own account and his or her own fiat currency. There is no exchange because most fiat ATMs are unable to transmit funds to third parties or accounts at other financial institutions.³⁶ Bitcoin ATMs, however, are not merely an intermediary between a consumer and his or her personal bank account. Bitcoin ATMs function as either one-way (converting fiat currency to Bitcoin) or two-way (converting fiat currency to Bitcoin and Bitcoin to fiat currency) machines. In both instances, these machines may act as intermediaries between buyers and sellers – more as a broker than as a teller. Therefore, Bitcoin ATM operators generally must register with FinCEN as money transmitters.

- **Internet casinos:** Internet casinos are virtual platforms that often accept bets and issue payouts denominated in CVC. Any internet casino that accepts and transmits value denominated in CVC may be regulated under the BSA as a money transmitter, and perhaps as a casino, another form of “financial institution” subject to BSA rules, in addition to any laws and regulations applicable to gambling.³⁷

Registering as a money services business

Persons engaged in money transmission have 180 days to register with FinCEN.³⁸ Any company or individual serving as an MSB must file a FinCEN Form 107, along with an estimate of business volume for the coming year, information related to the business’s ownership and control, and a list of its authorized agents.³⁹ FinCEN Form 107 requires MSBs to identify the states in which they have agents and branches, the type of money services activities they plan to carry out (i.e., money transmitter, currency dealer or exchanger, check casher), the number of agents they have authorized to carry out each activity, and the location (financial institution and account number) of their primary transaction account.⁴⁰ If accepted, registration must be renewed every two years. If there is any change in ownership or control, transfer of a 10% voting or equity interest, or more than a 50% increase in authorized agents, then the business must re-register.⁴¹

Willful failures to comply with the reporting, recordkeeping, and AML program requirements for money transmitters can result in penalties equal to the amount involved in any related transaction, up to \$229,269, or \$57,317, whichever is greater.⁴² The failure to maintain an appropriate AML program can result in a civil penalty of up to \$57,317 per day the violation persists. The U.S. Department of Justice prosecutes criminally willful violations of the BSA, and such violations can result in criminal fines of up to \$250,000 per violation, imprisonment for up to five years, or both.⁴³ It also is a felony to operate a money transmitter without required federal or state registrations or licenses.⁴⁴ While federal registration is relatively easy, once registered, ongoing BSA compliance obligations can be substantial.

No action letters/requests for rulings to federal or state regulators

If a person or entity is clearly a money transmitter, then federal registration with FinCEN is required, as is potential state licensing, as discussed below. However, there may be situations in which it is unclear whether a person or entity must register as a money transmitter. In such circumstances, a person may request an administrative ruling from FinCEN.⁴⁵ A positive determination that a particular business model is not subject to regulation under the BSA can be an important asset, but FinCEN can take a considerable amount of time to grant such a determination, and of course may reach a different result from what the business wanted.

State virtual currency money transmission

State money transmission, unlike federal money transmission, requires licensure, not registration. As a prerequisite to receiving a license and/or in connection with maintaining a license, states generally require some combination of the following: payment of licensing costs; bonding; minimum net-worth requirements; disclosure of applicants’ employment history; submission to investigations or examinations; audited financials and periodic financial reporting; prior money transmission or financial services business experience; disclosure of litigation and bankruptcy proceedings; and fingerprinting and background checks.

Importantly, even if a person or entity is not a money transmitter under the BSA, they may be a money transmitter in any number of states, or *vice versa*.

A license is required in any state where the person or company does business, or solicits citizens, regardless of whether he or she or it has any physical presence in the state. Thus, any entity that is planning a global or nationwide rollout of its virtual currency business must satisfy state licensing requirements regardless of where the entity is physically located. Because virtual currency is a borderless medium of exchange, this typically requires an analysis of, and possible licensure in, all 50 states in the U.S. and the District of Columbia.

Whether a particular entity is required to obtain a license in any state depends heavily on the specifics of the entity's business model. The below is meant to provide an overview of whether licensure may be required in a given state for entities engaged in certain virtual currency activities. For many states, we indicated that the state has taken no position on the applicability of its money transmission regulations to virtual currency businesses. However, in many of these states, a conservative reading of the definition of money (which is not necessarily limited to sovereign currency), monetary value (generally defined as "a medium of exchange, whether or not redeemable in money"), stored value (generally defined as "monetary value that is evidenced by an electronic record"), or a payment instrument (which generally includes "an electronic instrument or order for the transmission or payment of money whether or not the instrument is negotiable") would require a virtual currency business to obtain a license. In light of this, some virtual currency businesses have obtained a traditional money transmitter license in certain states. Any analysis of applicable licensure requirements is inherently fact-specific, necessitating a detailed application of an entity's business model to the particular statutes and guidance in any given state. Due to these intricacies of state money transmission law and the uncertain applications of such laws to virtual currency activities, we recommend that you consult with counsel when determining whether state licensure is required.

State-level analysis

Alabama: Requires a license to transmit virtual currencies because virtual currencies are considered "monetary value" which is subject to regulation.⁴⁶

Alaska: Requires virtual currency money transmitters to enter into a Limited License Agreement with the Alaska Department of Commerce, Community and Economic Development, Division of Banking and Securities.⁴⁷

Arizona: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁴⁸ In 2018, Arizona established a regulatory sandbox for the purpose of "enabl[ing] a person to obtain limited access to the market in this state to test innovative financial products or services without obtaining a license or other authorization that otherwise might be required."

Arkansas: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁴⁹

California: The California Department of Business Oversight ("CDBO") released several opinion letters in 2019 and 2020 covering virtual currency.⁵⁰ Many of the opinions reflect that the CDBO has not yet determined whether virtual currencies are a form of money that triggers the application of the California Money Transmission Act and whether companies that deal in virtual currency need to be licensed and supervised. The opinion letters apply to various virtual currency businesses including virtual currency escrow accounts and exchanges, virtual currency ATMs, virtual currency exchange platforms, companies seeking to receive virtual currency donations, and mobile-payments networks that allow consumers to use virtual currencies to pay for goods and services in California. The opinion letters are fact-specific and caution should be used in relying upon them. California Assembly

Bill 1489, the Uniform Regulation of Virtual-Currency Business Act (“URVCBA”), was introduced by the legislature but has not been passed.⁵¹

Colorado: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.⁵²

Connecticut: Requires a license to transmit virtual currencies.⁵³

Delaware: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁵⁴

District of Columbia: The District has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁵⁵

Florida: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.⁵⁶ In addition, in January 2019, in *State v. Espinoza*, 264 So. 3d 1055 (Fla. Dist. Ct. App. 2019), a Florida appellate court ruled that the state’s money transmitter laws apply to a business engaging in the sale of Bitcoin because Bitcoin is a “payment instrument.”

Georgia: Requires a license to transmit virtual currencies.⁵⁷

Hawaii: Requires a license to transmit virtual currencies.⁵⁸ SB2594 was introduced to the legislature in January 2020 with bipartisan backing, which would make it legal for Hawaiian banks to hold “digital securities,” “virtual currencies,” “digital consumer assets” and other “open blockchain tokens” for their customers. It would further authorize Hawaiian courts to hear digital asset claims. In August 2020, Hawaii announced that 12 virtual currency firms were selected to pilot Hawaii’s digital currency regulatory sandbox that allows virtual asset service providers to do business in the state without obtaining a money transmitter license for a two-year period. The pilot program is offered through the Digital Currency Innovation Lab, a partnership between Hawaii’s Department of Financial Institutions and the Hawaii Technology Development Corporation.

Idaho: Entities that operate an exchange or trade platform that allows users to exchange one digital currency for another, but that do not allow trading in or deposits of fiat currency, do not require a license; an entity that sells its own inventory of virtual currency does not require a license, but an entity that holds customer funds while arranging an exchange with a third party and that transmits virtual currency between the parties does require a license.⁵⁹

Illinois: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.⁶⁰

Indiana: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.⁶¹

Iowa: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁶²

Kansas: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.⁶³

Kentucky: The commonwealth has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁶⁴

Louisiana: On June 13, 2020, the Louisiana governor signed HB 701, which provides for the licensing and regulation of virtual currency businesses in the state. Subject to certain exceptions, the bill establishes licensing and registration requirements, and, among other things: (i) authorizes reciprocity of licensure with other states; (ii) specifies that licensee applications must be submitted through the Nationwide Multi-State Licensing System;

(iii) adds provisions related to licensee examinations; (iv) outlines licensee surety bond requirements “based on the nature and extent of risks in the applicant’s virtual currency business model;” (v) provides the state’s office of financial institutions with enforcement authority; and (vi) prohibits licensees from engaging in unfair, deceptive, or fraudulent practices. The act became effective on August 1, 2020.⁶⁵

Maine: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁶⁶

Maryland: The state has suggested that it generally does not regulate virtual currency at this time.⁶⁷

Massachusetts: The commonwealth generally does not regulate domestic money transmission. The state also exempts Bitcoin ATMs from “financial institution” and Bitcoins from foreign currency transmission regulations.⁶⁸ Businesses involved in the dissemination of virtual currencies on the internet are “marketplace facilitators” subject to sales or use tax collection.⁶⁹

Michigan: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter. Virtual currency transactions are exempt from sales tax, and retailers are required to instantly convert the value of the virtual currency to U.S. Dollars as of the day and the exact time of the transaction.⁷⁰

Minnesota: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁷¹

Mississippi: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁷²

Missouri: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter, except that it exempts Bitcoin ATM transactions from sales tax.⁷³

Montana: The state is the only U.S. jurisdiction that does not regulate money transmission.

Nebraska: The state has taken no current position on virtual currency money transmission as of the date of publication of this chapter.

Nevada: Bitcoin ATM kiosks must be licensed by the state and will require a surety bond requirement.

New Hampshire: The state exempts from licensure “persons who engage in the business of selling or issuing payment instruments or stored value solely in the form of convertible virtual currency or receive convertible virtual currency for transactions to another location.”⁷⁴

New Jersey: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁷⁵

New Mexico: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.⁷⁶

New York: A license (known as the BitLicense) is required by the New York State Department of Financial Services (“NYDFS”) to engage in any “Virtual Currency Business Activity,” which is broadly defined under the regulations, but has certain significant exemptions.⁷⁷ On June 24, 2020, NYDFS launched a proposed conditional licensing framework, final guidance concerning a licensee’s ability to self-certify the use of new coins, and additional resources intended to help virtual currency market participants. NYDFS also requested comments on the proposed conditional licensing framework, which will allow an entity to apply for a conditional license when partnering with an existing NYDFS-authorized entity to engage in virtual currency business activity during the term of the conditional license.

North Carolina: Requires a license to transmit virtual currency.⁷⁸

North Dakota: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.⁷⁹

Ohio: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.

Oklahoma: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter. In 2019, HB 1954, the URVCBA, was introduced by the legislature, but has not been passed.

Oregon: Requires a license to transmit virtual currency.⁸⁰

Pennsylvania: The Pennsylvania Department of Banking and Securities has published guidance stating that virtual currency, including “Bitcoin,” is not considered “money” under the state’s Money Transmitter Act (“MTA”). Only “fiat currency,” or currency issued by the U.S. government, is considered “money” under the MTA and to transmit money under the MTA, (i) fiat currency must be transferred with or on behalf of an individual to a third party, and (ii) the money transmitter must charge a fee for the transmission. Because virtual currency trading platforms (along with virtual currency kiosks, ATMs, and vending machines) never directly handle fiat currency and there is no transfer of money from a user to a third party, they are not money transmitters under the MTA and therefore do not need a license in order to operate in the state.⁸¹

Rhode Island: HB 5847 was signed into law effective January 1, 2020, which adds virtual currency to the existing electronic money transmission and sale of check license law and adds additional provisions clarifying the licensing process. The bill renames Chapter 19-14.3 of Rhode Island’s General Laws titled “Sale of Checks and Electronic Money Transfers” to “Currency Transmission” and includes virtual currency within the definition of currency transmission. The bill defines virtual currency as a “digital representation of value that: (A) [i]s used as a medium of exchange, unit of account, or store of value; and (B) [i]s not legal tender, whether or not denominated in legal tender.” Among other things, the bill excludes from the definition of virtual currency a “[n]ative digital token used in a proprietary blockchain service platform.” Subject to certain exceptions, the bill requires a person engaging in currency transmission business activity to be licensed with the state. Additionally, the bill, among other things: (i) requires virtual currency licensees to provide resident users of their services specified disclosures; (ii) subjects applicants and licensees to mandatory compliance programs and monitoring; and (iii) prohibits licensees from engaging in unfair, deceptive, or fraudulent practices. The act is effective as of January 1, 2020.⁸²

South Carolina: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter, but the South Carolina Attorney General has published frequently asked questions that disclose that further guidance with respect to the transmission of virtual currencies will be provided in the “near future.”⁸³

South Dakota: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.

Tennessee: Tennessee guidance provides that transactions solely involving exchanges of cryptocurrency are not money under the Tennessee Money Transmitter Act. Even the exchange of cryptocurrency for sovereign currency or the exchange of one cryptocurrency for another between two parties is not money transmission. However, the exchange of cryptocurrency for sovereign currency through a third-party exchanger is generally considered money transmission. In addition, cryptocurrency ATMs may be considered money transmission under certain circumstances.⁸⁴

Texas: The state has taken the position that certain virtual currency money transmission activities do not require licensure while other transactions, including those involving virtual currency ATMs, may require licensure.⁸⁵

Utah: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter. In late 2019, Utah's governor signed into law HB 378, which created a sandbox program for companies providing "innovative financial products or services" in the state. Utah's sandbox allows participants to "temporarily test innovative financial products or services on a limited basis without otherwise being licensed or authorized to act under the laws of the state." The program is administered by the Utah Department of Commerce. Importantly, HB 378 specifically includes "blockchain technology" within its scope.⁸⁶

Vermont: Requires a license to transmit virtual currency.⁸⁷

Virginia: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.⁸⁸

Washington: Requires a license to transmit virtual currency.⁸⁹

West Virginia: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.⁹⁰

Wisconsin: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency under certain circumstances.⁹¹

Wyoming: The state exempts buying, selling, issuing, or taking custody of payment instruments or stored value in the form of virtual currency or receiving virtual currency for transmission from the Wyoming money transmitter licensure requirements.⁹² In addition, in 2019, the Wyoming legislature enacted HB 57, which created a financial technology sandbox for the testing of innovative financial products and services in Wyoming. An "innovative financial product or service" is defined as a product or service that uses "new or emerging technology, or new uses of existing technology, that provides a product, service, business model or delivery mechanism to the public and has no substantially comparable, widely available analogue in Wyoming, including blockchain technology." Wyoming's sandbox is tailored to allow individuals and companies with new ideas to bring their product or service to market in a supportive environment that facilitates collaboration, consumer protection and innovation.⁹³

Attempts to standardize licensing practices

The URVCBA establishes a regulatory structure for businesses engaging in, or offering to residents of enacting states, certain virtual-currency transfer, exchange, or custodial services. The URVCBA provides certainty and protections that will enable such businesses to operate to everyone's benefit. It includes provisions to enable start-up companies offering virtual-currency services room to test products and operate prior to full licensure without violating state "money transmitter" or "money services" laws or risking federal prosecution for being unlicensed under 18 U.S.C. Section 1960.⁹⁴ The URVCBA has not been adopted although, as noted above, a few states are considering its adoption.

In July of 2018, the Office of the Comptroller of the Currency ("OCC") announced that non-depository fintech firms engaged in a core banking function may apply for a special purpose national bank charter (the Fintech Charter). Businesses with this charter may conduct some financial service activities without state licenses, but will be subject to supervision and examination by the OCC. The Fintech Charter was promptly met with litigation from state

and local government regulators in both New York and Washington, D.C., each of which raised similar legal challenges to the Fintech Charter.⁹⁵ The Washington, D.C. case was dismissed and the New York case is on appeal to the Second Circuit in New York. To date, no company has applied for a charter, perhaps due to the uncertainty created by these pending legal challenges.

In July 2020, Acting Comptroller of the Currency, Brian Brooks, told various media outlets that the OCC plans to introduce a special purpose national bank charter (the Payment Charter) that would give payment companies a nationwide servicing platform and federal preemption of state laws regarding licensing and regulation of money transmitters and payment services providers. The Payment Charter would be rolled out in two phases: first, a basic national money-transmitter license; second, direct access to the Federal Reserve's payments system, giving payment companies the ability to clear payments through the Federal Reserve System. As of the publication of this chapter, no additional information regarding the proposed Payment Charter was available.

In an attempt to simplify the process and to create some uniformity and efficiency, seven states—Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington—have come together to reach a level of reciprocity.⁹⁶ In early 2018, these states agreed that if one party state reviews key requirements of state licensing for a money transmitter applicant, including cybersecurity, background checks, and compliance with the BSA, then the other participating states will accept those findings in their own licensing process. This is the first real step toward an integrated 50-state system of licensure and supervision.

Most recently, on September 15, 2020, the Conference of State Bank Supervisors (“CSBS”) announced the launch of a “state-initiated program whereby nationwide payments firms will undergo a single comprehensive exam to satisfy all state regulatory requirements.” The new regulatory regime will streamline licensing and ongoing compliance for MSBs operating in 40 or more states by requiring MSBs to undergo a single exam by a joint group of state regulators. The CSBS’s new regulatory regime is intended to make it easier for MSBs to operate across multiple states.⁹⁷

* * *

Endnotes

1. 12 U.S.C. 1829b, 12 U.S.C. 1951–1959, 18 U.S.C. 1956, 18 U.S.C. 1957, 18 U.S.C. 1960, and 31 U.S.C. 5311–5314 and 5316–5332.
2. FinCEN does not have criminal enforcement authority.
3. 31 U.S.C. §§ 5311–5332.
4. *See, e.g.*, 31 C.F.R. §§ 1020.320 (SAR requirement for banks); 1022.320 (SAR requirement for MSBs).
5. *See, e.g.*, 31 C.F.R. § 1020.320(a)(2)(iii); *cf.* Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual (2014), at Appendix F.
6. *See, e.g.*, 31 C.F.R. §§ 1020.210(b)(5) (CDD requirement); 1020.220 (CIP requirement).
7. *See* 31 C.F.R. § 1022.380.
8. 31 C.F.R. § 1010.100(ff)(5).
9. 31 C.F.R. § 1010.100(ff)(5)(i).
10. *See* 76 Fed. Reg. 43585, 43586, 43588 (July 21, 2011).
11. FinCEN, FIN-2013-G001 (Mar. 18, 2013) (“2013 Guidance”), at 1.

12. *Id.*
13. 2013 Guidance at 1.
14. 2013 Guidance at 4.
15. *Id.*
16. *Id.* at p. 2.
17. *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014).
18. *See also Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001 (Jan. 30, 2014) (clarifying that a user is a person who obtains virtual currency to purchase goods or services on the user's own behalf).
19. *Id.* at p. 2.
20. FIN-2013-G001 p. 2.
21. *See also* <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-keneth-blanco-delivered-2018-chicago-kent-block>.
22. 31 C.F.R. § 1010.100(ff)(5)(ii)(A).
23. *See Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform*, FIN-2014-R011 (Oct. 27, 2014).
24. 2014 Software and Investment Guidance p. 2.
25. 2014 Mining Guidance.
26. FIN-2013-G001 p. 4.
27. 31 C.F.R. § 1010.100(ff).
28. FinCEN pursued enforcement action against Eric Powers in April 2019 for operating a peer-to-peer exchange for virtual currency without registering with FinCEN as a money transmitter. Mr. Powers advertised his intent to buy and sell Bitcoin on the internet, and completed transactions by physical delivery, mail or coordinating wires. Numerous of these transactions were also suspicious. FinCEN also levied a \$35,000 fine against Mr. Powers and Mr. Powers agreed to an industry bar from providing money transmission services or other activity that would make him a money service business for purposes of FinCEN regulation.
29. 31 C.F.R. § 1010.100(ff)(8)(iii).
30. *See* FIN-2014-R002 (concerning the regulatory treatment of those persons investing in CVCs).
31. 2019 Guidance at 26; *see also* Letter from Drew Maloney, Assistant Secretary for Legislative Affairs, U.S. Department of the Treasury, to Senator Ron Wyden (Feb. 13, 2018) (explaining with respect to ICOs “that a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency, is a money transmitter”).
32. 2014 Payment System Ruling.
33. *Id.*
34. 2014 Payment System Ruling p. 3.
35. *Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services*, FIN-2007-G006 (Dec. 3, 2007).
36. *Id.*
37. Definition of “financial institutions” to include casinos at 1010.100(t).
38. 31 C.F.R. § 1022.380.
39. 31 C.F.R. § 1022.380.
40. *See* FinCEN Form 107 (Mar. 2011).
41. 31 C.F.R. § 1022.380(b)(4).

42. 31 U.S.C. 5321; 84 Fed. Reg. 54495, 54496 (Oct. 10, 2019).
43. 18 U.S.C. § 1960.
44. *See* 18 U.S.C. § 1960(b)(1)(A), (B).
45. *See* 31 C.F.R. § 1010.711.
46. Ala. Code § 8-7A-1 *et seq.* (2017).
47. *See* <https://www.commerce.alaska.gov/web/dbs/LimitedLicenseAgreementOrders.aspx> (last visited Sept. 14, 2020).
48. Ariz. Rev. Stat. Ann. § 6-1201 *et seq.* (2014); A.R.S. §§ 41-5601 to 41-5612 (2018).
49. Ark. Code Ann. § 23-55-101 *et seq.* (West 2008).
50. *See* <https://dbo.ca.gov/dfi-opinion-letters/>.
51. In February 2019, Assembly Bill 1489 was introduced to the California legislature to enact the “Uniform Regulation of Virtual-Currency Business Act” which provides a statutory framework for the regulation of companies engaging in “virtual currency business activity,” such as exchanging, transferring, or storing virtual currency, or exchanging digital representations of value within online games for virtual currency or legal tender. The bill has not been passed.
52. Colo. Rev. Stat. § 11-110-106 *et seq.* (West 2017); *see also* Interim Regulatory Guidance Cryptocurrency and the Colorado Money Transmitters Act, Colorado Department of Regulatory Agencies, Sept. 20, 2018, <https://blockchainlawguide.com/resources/2018-09-20---Interim-Regulatory-Guidance-Cryptocurrency-and-the-Colorado-Money-Transmitters-Act.pdf>.
53. Conn. Gen. Stat. Ann. § 36a-595 *et seq.* (2013).
54. *See generally* De. Code Ann. tit. 5, § 2303 (West 2020).
55. *See generally* D.C. mun. Regs. tit. 26 ch. 26C22 *et seq.* (2020).
56. Fla. Stat. § 896.101 *et seq.* (West 2017); *see also* Florida Declaratory Statement No. 2018-538, 91969 (Nov. 19, 2018).
57. Ga. Code Ann. § 7-1-680 *et seq.* (West 2020).
58. Haw. Rev. Stat. Ann. § 489D-1 *et seq.* (West 2006); *see also* Hawaii Division of Financial Institutions News Release: State Warns Consumers on Potential Bitcoin Issues, Feb. 26, 2014, *available at* <https://cca.hawaii.gov/dfi/news-releases/news-release-state-warns-consumers-on-potential-bitcoin-issues/> (last visited Sept. 15, 2020). Coinbase exited Hawaii in 2017, requiring Hawaiian customers to close their accounts, stating that it would be impossible for Coinbase to operate in the state given the reserve requirement for money transmitters in the statute.
59. Idaho Department of Finance, Letter Dated March 12, 2018, *available at* <https://www.finance.idaho.gov/legal/no-action-opinion-letters/money-transmitter/documents/digital-currency/2018-03-09.pdf>.
60. 205 Ill. Comp. Stat. Ann. § 657/1 *et seq.* (West 1995); *see also* Illinois Department of Financial and Professional Regulation, Digital Currency Regulatory Guidance (June 13, 2017), *available at* <https://www.idfpr.com/Forms/DFI/CCD/IDFPR%20-%20Digital%20Currency%20Regulatory%20Guidance.pdf>.
61. Ind. Code § 28-8-4-1 *et seq.* (2013); *see also* Money Transmitter License New Application Checklist, Ind. Dep’t of Fin. Inst., *available at* <http://nationwidelicensing.system.org/slr/PublishedStateDocuments/IN-DFI-Money-Transmitter-Company-New-App-Checklist.pdf> (last updated March 10, 2020).
62. *See generally*, Iowa Code § 533C.102 *et seq.* (2003).
63. Kan. Stat. Ann. § 9-508 *et seq.* (West 2017). *See Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act*, Kan. Off of the State Bank

- Comm'r (June 6, 2014), *available at* http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf.
64. *See generally* Ky. Rev. Stat. Ann. § 286.11-001 *et seq.* (West 2006).
65. HB 701, 2020 Reg. Sess. (La. 2020), codified at La. R.S. §§ 6:1381 to 6:1394 (eff. Aug 1, 2020).
66. *See generally* Me. Rev. Stat. tit. 32, § 6101 *et seq.* (1997).
67. Md. Code Ann., Fin. Inst. § 12-401 *et seq.* (West 2014); *see Virtual Currencies: Risk for Buying, Selling, Transacting, and Investing – Advisory Notice 14-01*, Off. of the Comm'r of Fin. Regulation (Apr. 24, 2014), *available at* <https://www.dllr.state.md.us/finance/advisories/advisoryvirtual.pdf>.
68. Mass. Division of Banks, Opinion 14-004 (May 12, 2014). 63. 830 CMRH 1.7(b)(1), *available at* <https://www.mass.gov/doc/selected-opinion-14-004/download> (last visited Sept. 15, 2020).
69. Mass. Gen. Laws ch. 169, § 1 *et seq.* (West 1991); *see* Mass. Div. of Banks, Opinion 18-003 (June 14, 2018), *available at* <http://www.mass.gov/files/documents/2018/06/21/Select%20Opinion%2018-003.pdf> (last visited Sept. 15, 2020).
70. *See* Tax Policy Division of the Michigan Dept. of Treasury, Treasury Update, Vol. 1, Issue 1 (November 2015), *available at* https://www.michigan.gov/documents/treasury/Tax-Policy-November2015-Newsletter_504036_7.pdf (last visited Sept. 14, 2020).
71. *See generally* Minn. Stat. § 53B.01 *et seq.* (2001).
72. *See generally* Miss. Code Ann. § 75-15-1 *et seq.* (West 2010).
73. Missouri Dep't of Revenue, LR 7411, Collection of Sales Tax on Bitcoin Transfers Through an Automated Teller Machine (ATM), (Sept. 12, 2014), *available at* <http://dor.mo.gov/rulings/show/7411> (last visited Sept. 15, 2020).
74. N.H. Rev. Stat. Ann. § 399-G:3 (2017).
75. *See generally* N.J. Stat. Ann. § 17:15C *et seq.* (1998).
76. N.M. Stat. Ann. § 58-32-101 *et seq.* (West 2017); *see also* *Money Service Business: FAQ's*, N.M. Reg. & Licensing Dep't, *available at* <http://www.rld.state.nm.us/financialinstitutions/faq-s.aspx>.
77. 23 N.Y. Comp. Codes R. & Regs § 200. The New York State regulatory scheme has been the subject of much criticism and has resulted in an exodus of businesses from New York because of the costs and regulatory requirements associated with the BitLicense. As of the date of this chapter, 18 companies have been granted a BitLicense. *See also* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202006241 (last visited Sept. 15, 2020).
78. N.C. Gen. Stat. § 53-208.41 *et seq.* (2016).
79. N.D. Cent. Code § 13-09-01 *et seq.* (West 2005). *See Frequently Asked Questions – Non-Depository: Money Transmitters*, N.D. Dep't of Fin. Insts. (2018), <https://www.nd.gov/dfi/about-dfi/non-depository/frequently-asked-questions-non-depository>.
80. Or. Rev. Stat. Ann. § 717.205 *et seq.* (West 2018).
81. *Money Transmitter Act Guidance for Virtual Currency Businesses*, Pa. Dep't of Banking and Secs. (Jan. 2019).
82. *See* R.I. HB 5847 (2019).
83. *See* South Carolina Attorney General, *Money Services Frequently Asked Questions*, *available at* <http://www.scag.gov/money-services-frequently-asked-questions> (last visited Sept. 14, 2020).
84. *See* Memo, Tenn. Dep't of Fin. Inst., *Regulatory Treatment of Virtual Currencies under the Tennessee Money Transmitter Act* (Dec. 16, 2015), *available at* <https://www>.

- tn.gov/content/dam/tn/financialinstitutions/new-docs/TDFI%20Memo%20on%20Virtual%20Currency.pdf (last visited Sept. 14, 2020).
85. See Texas Dep't of Banking, Supervisory Memorandum 1037, *Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act*, available at <https://www.dob.texas.gov/sites/default/files/files/consumer-information/sm1037.pdf> (last visited Sept. 14, 2020).
 86. See <https://commerce.utah.gov/sandbox.html>.
 87. Vt. Stat. Ann. tit. 8, § 2500 *et seq.* (West 2019).
 88. Va. Code Ann § 6.2-1900 *et seq.* (West 2019); see also Va. State Corp. Comm., *Notice to Virginia Residents Regarding Virtual Currency*, available at <https://www.scc.virginia.gov/getattachment/1bb52b42-9a10-45a2-ba48-b352e48b6d2e/virtcur.pdf> (last visited Sept. 14, 2020).
 89. Wash. Rev. Code § 19.230.010 *et seq.* (West 2017).
 90. W. Va. Code § 61-15-1 *et seq.* (West 2017).
 91. Wis. Stat. § 217.01 *et seq.* (West 2019); see also <https://www.wdfi.org/fi/lfs/soc/> (last visited Sept. 14, 2020).
 92. Wyo. Stat. Ann., § 40-22-101 *et seq.* (West 2003); see also <http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/financial-technology-sandbox>.
 93. <http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/financial-technology-sandbox>.
 94. See <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=de52d1fe-1f70-a568-9552-d354ade157ca&forceDialog=0>.
 95. See *Lacewell v. Office of the Comptroller of the Currency*, Case 1:18-cv-08377-VM (S.D.N.Y.) (ECF No. 45); *Conference of State Bank Supervisors v. Office of the Comptroller of the Currency*, No. 18-cv-2449 (DLF) (D. D.C.).
 96. See Conf. of State Bank Supervisors, *State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments*, (Feb. 6, 2018), available at <https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments> (last visited Sept. 14, 2020).
 97. *State Regulators Roll Out One Company, One Exam for Nationwide Payments Firms* (Sept. 15, 2020), available at <https://www.csbs.org/regulators-announce-one-company-one-exam-for-payments-companies>.

* * *

Acknowledgments

The authors acknowledge with thanks the contributions to this chapter by Nicole Succar and Jorge Pesok.

**Michelle Ann Gitlitz****Tel: +1 212 895 4334 / Email: mgitlitz@crowell.com**

Michelle Gitlitz is the Global Head of Crowell & Moring's Blockchain and Digital Assets practice, and a partner in the White Collar and Regulatory Enforcement and Corporate groups. An experienced regulatory lawyer and litigator, Michelle's practice focuses on the legal and regulatory issues facing both emerging and established companies that invest in and incorporate blockchain technology and digital assets into their businesses. Her experience includes: advising clients on the legal, regulatory, and risk management issues surrounding coin/token offerings (including launching new offerings and remediating prior offerings); working with clients in connection with digital currency exchanges and platforms; establishing new blockchains and nodes; and advising clients on navigating federal and state money transmission laws.

**Carlton Greene****Tel: +1 202 624 2818 / Email: cgreene@crowell.com**

Carlton Greene is a partner in Crowell & Moring's Washington, D.C. office and a member of the firm's International Trade and White Collar & Regulatory Enforcement groups. He provides strategic advice to clients on U.S. economic sanctions, Bank Secrecy Act and anti-money laundering (AML) laws and regulations, export controls, and anti-corruption/anti-bribery laws and regulations. Carlton is the former chief counsel at FinCEN (the Financial Crimes Enforcement Network), the U.S. AML regulator responsible for administering the Bank Secrecy Act. Before joining FinCEN, Carlton previously served as the assistant director for transnational threats with the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), where he directed targeting and investigations for more than 15 U.S. economic sanction programs, including those related to Iran and North Korea. Carlton also served as legal counsel to OFAC on counterterrorism sanctions.

**Caroline Brown****Tel: +1 202 624 2509 / Email: cbrown@crowell.com**

Caroline E. Brown is a partner in Crowell & Moring's Washington, D.C. office and a member of the firm's White Collar & Regulatory Enforcement and International Trade groups. She provides strategic advice to clients on national security matters, including anti-money laundering (AML) and economic sanctions compliance and enforcement challenges, cybersecurity, cross-border data transfers, and investigations. Caroline also advises companies navigating review by the Committee on Foreign Investment in the United States (CFIUS). Caroline brings over a decade of experience as a national security attorney at the U.S. Departments of Justice and the Treasury. Most recently, she served as an Attorney-Advisor in the Treasury Department's Financial Crimes Enforcement Network (FinCEN), where she developed an in-depth understanding of AML regulation and enforcement and FinCEN's role in guarding the U.S. financial system against money laundering and terrorist financing.

Crowell & Moring LLP

590 Madison Avenue, 20th Floor, New York, NY 10022-2544, USA
Tel: +1 212 223 4000 / Fax: +1 212 223 4134 / URL: www.crowell.com

Cryptocurrency compliance and risks: A European KYC/AML perspective

Fedor Poskriakov, Maria Chiriaeva & Christophe Cavin
Lenz & Staehelin

Introduction

The rapid development, increased functionality, and growing adoption of new technologies and related payment products and services globally continue to pose significant challenges for regulators and private sector institutions in ensuring that these technologies are not misused for money laundering (“ML”) and financing of terrorism (“FT”) purposes. The underlying reasons for this are numerous and some of such risks were identified and discussed already in 2013 in the Financial Action Task Force (“FATF”) NPPS Guidance,¹ even though the said report did not specifically refer to “virtual currencies” at the time.

In the last couple of years, a significant number of virtual currencies and other virtual assets (“VAs”) have emerged and at least some of them attracted significant investment in payment infrastructures built on the relevant software protocols. These payment infrastructures and protocols seek to provide a new method for transmitting value over the internet or through decentralised peer-to-peer networks.

As decentralised, convertible cryptography-based VAs and related payment systems are gaining momentum, regulators and financial institutions (“FIs”) around the world are recognising that VAs and the underlying consensus protocols (1) likely represent the future for payment systems, (2) provide an ever-more powerful new tool for criminals, terrorist financiers and other sanctions-evaders to move and store illicit funds, out of the reach of law enforcement, and, as a result, (3) create unique new challenges in terms of ML/FT risks.² Although the global volumes and estimates are relatively low, Europol estimated in 2017 that 3–4% of Europe’s crime proceeds were laundered through cryptocurrencies – the proportion will likely continue to increase rapidly³ due to the rate of adoption of VAs, including by institutional investors and FIs.

Given the trans-jurisdictional (or borderless) nature of the VA phenomenon, major institutions at the international level have all focused on and issued reports addressing VAs and the risks associated with them, including ML/FT risks. FATF and the European Banking Authority (“EBA”), in particular, have issued recommendations in this context, concluding that VA exchange platforms allowing the conversion of VAs into fiat money (and *vice versa*) are of particular relevance and must be brought within the scope of the respective national anti-money laundering and counter-financing of terrorism (“AML/CFT”) frameworks. In June 2019, FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving VAs and certain virtual asset service providers (“VASPs”). More recently, FATF concluded that the revised standards on AML/CFT designed to specifically address VAs also apply to stablecoins.

Key potential risks

Key definitions and concepts

(a) *Definitions*

There is no single global definition of the term “crypto- or virtual currency”. In 2012, the European Central Bank (“**ECB**”) defined virtual currencies as “*a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*”.⁴ In 2014, the EBA defined virtual currencies as a “*digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a [fiat currency], but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*”.⁵ In its 2014 report on key definitions on virtual currencies, FATF first gave the following definition: “[T]he digital representation of value that can be digitally traded and functions as: (i) a medium of exchange; and/or (ii) a unit of account; and/or (iii) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.”

In order to provide for a common regulatory approach through the fifth Anti-Money Laundering Directive (“**MLD5**”, see also “Current legal and regulatory regime, MLD5”, below), the EU decided to adopt a definition of virtual currencies deriving from FATF’s 2014 guidance. According to MLD5, a virtual currency is defined as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically. Given the broad nature of this definition, it is likely that, in practice, most forms of VAs and other transferable cryptographic coins or tokens (as we know them today) fall within the scope of MLD5.

Finally, FATF updated its Recommendations in October 2018 and introduced the definition of VAs, now defined as a “*digital representation of value that can be physically traded, or transferred, and can be used for payment or investment purposes*” (but do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations).⁶ In its June 2020 report on stablecoins, FATF further concluded that stablecoins could either be classified as VAs or traditional financial assets under the revised FATF standards.⁷

For the purposes of this chapter, we will adopt the definitions and conceptual framework set out in FATF’s updated Recommendations.⁸ In this respect, we will focus on decentralised convertible VAs and related payment products and services (“**VCPPS**”), to the exclusion of other VA-related securities and/or derivatives products and services, even though these are also relevant for ML/FT risk assessment, in particular crowdfunding methods like initial coin offerings (“**ICOs**”).

(b) *KYC and transaction monitoring*

Know Your Customer (“**KYC**”) is the cornerstone of the AML/CFT due diligence requirements that are generally imposed on FIs whose AML/CFT legislation is aligned with international standards. KYC requirements are relatively recent, as they were first implemented in the 70s in both Swiss and US legislation, before becoming an internationally recognised concept through the issuance of the FATF Recommendations. KYC requires that FIs duly identify (and verify) their contracting parties (i.e.,

customers) and the beneficial owners (namely when their contracting parties are not natural persons) of such assets, as well as their origin. Together with transaction monitoring, KYC ensures the traceability of assets, as long as those remaining in the financial system (i.e., paper trail), and allows the identification of ML/FT indicia.

Although KYC and transaction-monitoring requirements were globally implemented at a time when VAs did not exist, it appears today, based on the various initiatives both at the international and national levels, that the application of AML/CFT requirements to VCPSS remains to be clarified.

One of the challenges is that KYC and other AML/CFT requirements were designed for a centralised intermediated financial system, in which regulatory requirements and sanctions can be imposed by each jurisdiction at the level of financial intermediaries operating on its territory (i.e., acting as “gatekeepers”). By contrast, VCPSS rely on a set of decentralised cross-border virtual protocols and infrastructure elements, neither of which has a sufficient degree of control over or access to the underlying value (asset) and/or information, so that identifying a touchpoint for implementing and enforcing compliance with AML/CFT requirements is naturally challenging.

Potential AML/CFT risks

It has to be recognised that like any money-transmitting or payment services, VCPSS have legitimate uses, with prominent venture capital firms investing in VA start-ups and developing infrastructure platforms. VAs may, for example, facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the internet. VAs may also facilitate international remittances and support financial inclusion in other ways, so that VCPSS may potentially serve the under- and un-banked.

However, most VAs by definition trigger a number of ML/FT risks due to their specific features, including anonymity (or pseudonymity), traceability and decentralisation. Many of those risks and uses materialise not on the distributed ledger (“DL”) of the relevant VA, but rather in the surrounding ecosystem of issuers, exchangers and users. Rapidly evolving technology and the ease of new cryptocurrency creation are likely to continue to make it difficult for law enforcement and FIs alike to stay abreast of new criminal uses, so that integrating those in a solid KYC/client due diligence (“CDD”) framework is a never-ending task.

In addition to potential illicit uses of VCPSS, the use of VAs may facilitate ML by relying on the same basic mechanisms as those used with fiat currency, with a significant potential for abuse of unregulated and decentralised borderless networks underpinning VAs. In a nutshell:

- **Placement:** VAs offer the ability to open a significant number of anonymous or pseudonymous wallets, at no or very low cost, something that is a low-risk method of rapidly placing proceeds of illicit activity.
- **Layering:** VAs enable the source of funds to be obfuscated by means of multiple transfers from wallet to wallet and/or their conversion into different types of VAs across borders. This allows for an easy layering without significant cost or risk, it being understood that recent technological developments such as “atomic swaps” may even further facilitate the misuse of VAs. Incidentally, substantial demand for unregistered ICOs may allow criminals (assuming they control the ICO) to hijack the popular crowdfunding mechanism to convert VA proceeds into other VAs and/or fiat currencies, while adding a seemingly legitimate “front” for the source of funds.
- **Integration:** the use of VAs to acquire goods or services, either directly or through the conversion of the VAs into fiat currency, is facilitated by the ever-increasing list of goods and services for which payment in VAs is accepted, as well as the entry into

the VA markets of institutional players both for investment and trading (speculation) purposes, providing substantial liquidity in the VA markets and thereby potentially facilitating large-scale integration by abusing unsuspecting institution actors/investors. Likewise, ICOs with below-average KYC requirements may be abused by criminal actors who may be able to convert their illicit VA holdings into other tokens through subscribing to an ICO, and then exiting the investment immediately upon the relevant coins or tokens becoming listed on any VA exchange.

Naturally, AML/CFT risks are heightened among the unregulated sectors of the cryptocurrency markets. Given regulatory pressure to reject anonymity and introduce AML controls wherever cryptocurrency markets interface with the traditional financial services sector, there are new VAs being created to be more compatible with existing regulations.

However, until such time as novel technological solutions are in place, ML/FT risks are typically addressed by imposing strict AML/KYC requirements on “gatekeepers” such as VA exchangers and other FIs. However, according to the Impact Assessment of the European Commission of July 2016,⁹ depending on the evolution of the network of acceptance of VAs, there might come a point in time when there will no longer be a need to convert VAs back into fiat currency if VAs become widely accepted and used. This presents a critical challenge in itself, insofar as it will reduce the number of “touchpoints” (i.e., conversion points from VA to fiat, exchangers, etc.) with the traditional intermediated financial services sector and thereby limit the opportunities for ML/FT risk mitigation through regulation of defined intermediaries. The updated FATF Recommendations, however, significantly extended the scope of entities subject to AML/CFT regulation by ensuring that not only VA activities that intersect with and provide gateways to and from the traditional regulated financial system (in particular VA exchangers), but also crypto-to-crypto exchange platforms, ICO issuers, custodial wallets and other related service providers, are regulated for AML/CFT purposes (see “Current international initiatives, FATF”, below).

Anonymity/pseudonymity

By definition, decentralised systems are particularly vulnerable to anonymity risks. Indeed, in contrast to traditional financial services, VA users’ identities are generally unknown, although in most cases they are only pseudonymous, and there is no regulated intermediary that may serve as “gatekeeper” for mitigation of ML/FT risks.

The majority of VAs, such as *Bitcoin* (“*BTC*”) or *Ether* (“*ETH*”), have anonymity or pseudonymity by design. The user’s identity is not linked to a certain wallet or transaction. However, while a user’s identity is not visible on the relevant DL underpinning the VA infrastructure, information on transactions, such as dates, value and the counterparties’ addresses, are publicly recorded and available to anyone. For the purposes of their investigation and prosecution work, enforcement authorities are therefore able to track transactions to a point where the identity may have been linked to an account or address (e.g., wallet providers or exchange platforms).

Some VAs, such as Dash, Monero or Zcash and other “privacy coins”, even go further, as they are designed to be completely anonymous: wallet addresses, transactions and information on transactions are not publicly recorded on the relevant DL and provide for complete anonymity, preventing the identification of the legal and beneficial owner of the VAs.

In addition, a number of solutions have emerged that allow a certain enhancement of the anonymity and seek to limit traceability of transactions on otherwise pseudonymous VA networks. For instance, mixing services (also known as “*tumblers*” or “*washers*”) aggregate transactions from numerous users and enable the actual paper trail of the transactional

activity to be obscured. However, while the precise trail of individual transactions might be obscured, the fact that mixing activity has occurred is detectable on the relevant DL.

Traceability

Although the anonymous or pseudo-anonymous design of VAs is an obvious risk of ML/FT, the public nature of the DL acts as a mitigant by offering a complete transaction trail. The DL is an immutable, auditable electronic record of transactions whose traceability may, however, be limited due to user anonymity and anonymising service providers that obfuscate the transaction chain (see also “Technological solutions?”, below).

The traceability or “trail” risks may not be significant when dealing with a single DL or VA protocol. However, the situation becomes much more complex when considering cross-VA exchanges where it may not necessarily be possible to easily trace conversion transactions from one VA/DL to another, given that such tracing may require access to off-chain records of intermediaries or exchangers, which may be unregulated, and located in multiple jurisdictions. Likewise, with the emergence of technological solutions allowing for so-called “atomic swap”, or atomic cross-chain trading, traceability will become an even greater challenge. In essence, it will allow users to cross-trade different VAs without relying on centralised parties or exchanges.

Decentralisation

Most VAs are decentralised, i.e., they are distributed on a peer-to-peer basis and there is no need for validation by a trusted third party that centrally administers the system. As noted by FATF, law enforcement cannot target one central location or entity (administrator) for investigative or asset-seizure purposes, and customers and transaction records are typically held by different parties, in multiple jurisdictions, making it more difficult for law enforcement and regulators to access them.¹⁰

This problem is exacerbated by the rapidly evolving nature of the underlying DL technology and VCPSPS business models. Without proper safeguards in place, transition from a VCPSPS to the fiat financial system may be facilitated by unsuspecting VA exchangers and/or abused by complicit VCPSPS infrastructure providers who deliberately seek out jurisdictions with weak AML/CFT regimes or deficient implementation of related controls.

Legal and regulatory challenges

Current legal and regulatory regime

Despite calls for the adoption of global AML standards for VAs, no such uniform rules have yet emerged. However, we have seen some convergence toward the logical FATF view that VCPSPS should be subject to the same obligations as their non-VA counterparts. In this respect, the majority of European jurisdictions that have issued rules or guidance on the matter have typically concluded that the exchange of VA for fiat currency (including the activity of VA “exchanges”) is or should be subject to AML obligations.

Differences in national regulations include: (1) varying licensing requirements for VA exchangers and wallet services; (2) treatment of ICOs from an AML regulatory standpoint; and (3) the extent to which crypto-to-crypto exchange is treated differently from crypto-to-fiat exchange. In many cases, the regulatory status of these activities is either ambiguous or case-specific, and partially dependent on new legislation or regulation being adopted.

EU

VAs were first addressed at the EU level when the ECB published its VA report in October 2012. The ECB notably acknowledged that the degree of anonymity afforded by VAs can

present ML/FT risks. The ECB further suggested that regulation “would at least reduce the incentive for terrorists, criminals and money launderers to make use of these virtual currency schemes for illegal purposes”.¹¹

In July 2014, the EBA issued a formal opinion on VAs, indicating in particular that VAs present high risks to the financial integrity of the EU, notably due to potential ML/FT risks. In its January 2019 report,¹² however, the EBA noted that VA-related activity in the EU was regarded as relatively limited and that such activity does not appear to give rise to implications for financial stability.

MLD5

On July 5, 2016, the European Commission presented a legislative proposal to amend MLD4. The proposal was part of the Commission’s Action Plan against FT, announced in February 2016. It also responded to the “Panama Papers”¹³ revelations of April 2016.

MLD5 was adopted by the Parliament in plenary on April 19, 2018 and the Council of the European Union adopted it on May 14, 2018. It was formally published in the EU’s *Office Journal* on June 19, 2018 and entered into force on July 9, 2018. Member States had until January 10, 2020 to amend their national laws to implement MLD5. To date, most Member States have fully implemented MLD5, although some of those failed to transpose MLD5 completely within the original prescribed deadlines.

Among different objectives, MLD5 expressly aims at tackling FT risks linked to VAs. In this context, VA exchange platforms and custodian wallet providers have been added in the scope of MLD5. In order to allow competent authorities to monitor suspicious transactions involving VAs, while preserving the innovative advances offered by such currencies, the European Commission concluded that it is appropriate to include in the institutions subject to MLD4 (“obliged entities”) all gatekeepers that control access to VAs, and in particular, exchange platforms and wallet providers,¹⁴ as recommended by FATF in its guidance (see “Current international initiatives, FATF”, below).

(i) *Providers engaged in exchange services*

Interestingly, MLD5 extends EU AML requirements to “providers engaged in exchange services between virtual currencies and fiat currency”. As a result, most crypto-to-fiat (or fiat-to-crypto) exchanges will be covered by MLD5. However, crypto-to-crypto exchanges do not seem to be expressly covered by MLD5.

Notwithstanding this, it is still possible that certain crypto-to-crypto exchanges may fall within the scope of MLD5 if their activities are conducted by “obliged entities” for other reasons, such as custodian wallet services (see (ii) below). Further, crypto-to-crypto exchanges could still be regulated at Member State level, depending on how each Member State incorporates MLD5’s provisions into its national law, as well as the FATF Recommendations. Similarly, VA ATMs are not covered under MLD5, but some Member States have introduced more stringent rules that cover those activities.

(ii) *Custodian wallet providers*

Custodian wallet providers are defined entities that provide services to safeguard private cryptographic keys on behalf of customers, to hold, store and transfer VAs. The definition appears to only include wallet providers that maintain control (via a private cryptographic key) over customers’ wallets and the assets in it, in contrast to pure software (non-custodial) wallet providers that provide applications or programs running on users’ hardware (computer, smartphone, tablet, etc.) to access public information from a DL and access the network (without having access to or control over the user’s private keys).

Switzerland

The Swiss AML legislation does not provide for a definition of VAs, relying upon FATF's definition used in its 2014 report. That being said, since the revision of the Swiss Financial Market Supervisory Authority ("FINMA") AML Ordinance in 2015, exchange activities in relation to VAs, such as money transmitting (i.e., money transmission with a conversion of VAs between two parties), are clearly subject to AML rules. Before this revision took place, both FINMA and the Federal Council had already identified,¹⁵ on a risk-based approach, the increased risks associated with VA exchangers and the necessity for them to be subject to AML requirements. As such, Switzerland was a precursor in the implementation of this rule, which has now become standard.

In a nutshell, the purchase and sale of convertible VAs on a commercial basis, and the operation of trading platforms to transfer money or convertible VAs from a platform's users to other users, are subject to Swiss AML rules, including the so-called "travel rule". Before commencing operations, a provider of these kinds of services must become a member of a self-regulatory organisation ("SRO").

Because convertible VAs can facilitate anonymity and cross-border asset transfers, FINMA considers trading in it to have heightened ML/FT risks, requiring strict CDD, particularly as regards client identification, beneficial ownership and source-of-funds analysis.

The key AML/CFT compliance requirement, which represents a challenge to FIs providing VSPPS because of the very nature of currently existing VAs, is undoubtedly the "travel rule". This rule requires that information about the client and the beneficiary be transmitted with payment orders.¹⁶ Although no system currently exists at either a national or an international level (such as, for example, SWIFT for interbank transfers) for reliably transferring identification data for payment transactions on a DL, there are practical ways for FIs to still comply with this requirement; however, they are comparatively onerous and therefore severely limit the development of VCPSPS. Notwithstanding this, there are several industry initiatives that aim at developing a technical solution to reliable and standardised implementation of the "travel rule" requirements, such as OpenVASP or interVASP. Once some of those standards are vetted by AML regulators, it should be expected that more VCPSPS will be offered on the market and that it will become easier to combine the purely decentralised world of VAs and traditional intermediated financial services.

Managing compliance AML/CFT risks

Although there are developments on the regulatory front in terms of strengthening requirements applicable to VCPSPS providers, there has been little guidance by regulators to their respective domestic FIs as to how to approach KYC/CDD from an ML/FT risk assessment perspective when dealing with customers exposed to VA and VCPSPS risks, other than a recommendation to adopt a prudent, risk-based approach.

In practice, as with any new line of business, type of client or financial transaction, the central AML/CFT compliance questions for FIs will be whether they: (1) understand the relevant risks; (2) can reasonably manage them; and (3) have the knowledge, tools and resources to do so on an ongoing basis (including policies, procedures, training programmes, etc.). FIs that choose to serve the new types of clients in the VA ecosystem should elaborate and put in place specific policies and procedures to ensure that they are able to comply with their AML obligations despite the VA context.

The specifics of each set of requirements will depend on the type of business, client type and jurisdiction, as well as other factors. That being said, the ability of FIs to confirm the identity,

jurisdiction and purpose of each customer, as well as the assessment of the source of wealth and funds, is essential to the fulfilment of AML/CFT requirements. VCPSS actors as customers present specific challenges in each of these aspects, so that FIs must ensure that their policies and procedures allow them to perform these core functions with a degree of confidence that is at least equal to that which FIs would require for their traditional financial services.

Given the varying typology of VCPSS service providers, it is virtually impossible to draw up KYC/CDD standards, procedures and checklists that would be applicable universally. It is therefore understandable that regulators have not issued blanket guidance in this space. As the understanding of VCPSS and related AML/CFT risks evolves, it is likely that international standards and recommendations will emerge, and possibly compliance tools which will simplify the implementation thereof by FIs. In this respect, FIs, VCPSS providers, developers, investors, and other actors in the VA space should seek to develop technology-based solutions that will improve compliance and facilitate the integration of VCPSS with the existing financial system.

Possible avenues to address compliance concerns

Current international initiatives

FATF

(a) Virtual Currencies – Guidance for a risk-based approach (June 2015 Standards)

In June 2015, FATF issued specific guidance on virtual currencies, focusing on the points of intersection that provide gateways to the regulated financial system – *Guidance for a Risk-Based Approach: Virtual Currencies* (the “**Guidance**”). This Guidance derives from previous reports of FATF, namely the June 2014 *Virtual Currencies Report* and the FATF NPPS Guidance of June 2013.

In accordance with the cardinal risk-based approach principle, the Guidance provides for a certain number of clarifications on the application of the FATF Recommendations to entities involved in VCPSS.

FATF is of the view that domestic entities providing convertible VA exchange services between VA and fiat currency should be subject to adequate AML/CFT regulation in their jurisdiction, like any other FI, and be subject to prudential supervision. In this context, the distinction between centralised and decentralised VAs is a key aspect for the purposes of the risk assessment to be performed. FATF recommends that entities involved in convertible and decentralised VCPSS be subject to an enhanced due diligence process, as such activities are regarded as higher risk due to the inherent anonymity element and challenges to perform proper identification (i.e., the underlying protocols on which the major part of the decentralised VCPSS are currently based do not provide for the participants’ identification and verification) (see also “Anonymity/pseudonymity”, above).

It is important to note that FATF does not recommend prohibiting VCPSS. On the contrary, such prohibition could drive such activities underground and lead to a complete lack of visibility and control over them. As a result, in case of prohibition of VCPSS, FATF recommends implementing additional mitigation measures, taking also into account the cross-border element in their activities.

As regards transaction monitoring, FATF is of the view that countries must ensure that originator and beneficial owner information is always included when convertible VA exchangers conduct convertible VA transfers in the form of wire transfers. Certain *de minimis* thresholds may, however, be implemented in order to exclude lower risk transactions. Transaction monitoring remains a key risk mitigant in the convertible VA world, as long as a conversion of VAs occurs.

(b) FATF Recommendations

FATF updated its Recommendations in October 2018 to address the rapidly evolving risks related to VAs and to clarify how the FATF Recommendations apply in the case of financial activities involving VAs. The updated Recommendations specifically address and target VASPs, defined as any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between VAs and fiat currencies; (ii) exchange between one or more forms of VAs; (iii) transfer of VAs; (iv) safekeeping and/or administration of VAs or instruments enabling control over VAs; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a VA.

These new definitions significantly expand the scope of entities subject to AML/CFT regulation since the June 2015 Guidance by ensuring that VASPs (not only fiat-to-VA exchanges but also crypto-to-crypto exchange platforms, ICO issuers, custodial wallets and other related service providers) are regulated for AML/CFT purposes, as well as licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. That being said, the above-mentioned definitions remain somewhat vague, and their interpretations remain to be determined.

(c) Interpretive Note to Recommendation 15

FATF adopted an Interpretive Note to Recommendation 15 on June 21, 2019, setting out requirements for effective regulation, supervision and monitoring of VASPs. Under this note, VASPs should be licensed or registered and be subject to effective regulation and supervision to ensure that they take the necessary steps to mitigate AML/CTF risks. To this end, VASPs should (1) be supervised or monitored by a competent authority (not a self-regulatory body), which should conduct risk-based supervision or monitoring and have power to impose a range of disciplinary and financial sanctions, and (2) adopt a number of preventive measures to mitigate ML and FT risks (including but not limited to CDD, record-keeping, suspicious transaction reporting and screening all transactions for compliance with targeted financial sanctions). In particular, VASPs should conduct CDD for occasional transactions above a USD/EUR 1,000 threshold. According to Paragraph 7(b) of the Interpretive Note, VASPs should obtain and hold required and accurate originator and beneficiary information in relation to VA transfers, and share this information with beneficiary VASPs and counterparts, as well as competent authorities (often referred to as the "travel rule"). Further, the specific requirements relating to wire transfers (such as monitoring the availability of information, taking freezing actions and prohibiting transactions with designated persons and entities) as set out under Recommendation 16 would apply on the same basis to transfers of VAs.

The Interpretive Note finally highlights the need for international cooperation and information exchange to prevent and combat ML/FT risks associated with VAs.

While the "travel rule" has been a longstanding requirement for FIs internationally, the implementation of this requirement for VASPs to collect and transfer customer information during transactions will undoubtedly present a challenge considering the very nature of DL technologies. Indeed, whereas FIs rely on established interbank communication systems (such as SWIFT, TARGET or SIC) to move funds and share information, no established communication system yet exists for VASPs, and DL technologies – as they stand – usually only require a recipient address to effect a transfer, which renders difficult – if not impossible – ownership verification by VASPs and determination of whether the recipient address is managed by another obliged VASP or a non-custodial wallet which would fall outside the FATF Recommendations.

(d) Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019 Standards)

In June 2019, FATF published the *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, which builds upon FATF's June 2015 Standards on the risk-based approach to VAs and VASPs and is intended to help both national authorities in understanding and developing regulatory and supervisory responses to VA activities and VASPs, as well as to help VASPs in understanding their AML/CFT obligations. Under the risk-based approach and in accordance with Paragraph 2 of the Interpretative Note, countries should identify, assess, and understand the ML/FT risks in relation to VA financial activities or operations and VASPs and focus their AML/CFT efforts on potentially higher-risk VAs. Similarly, countries should require VASPs to identify, assess, and understand the ML/FT risks. Finally, in a report dated June 2020, FATF confirmed that the June 2019 Standards also apply to stablecoins, as they are to be considered either VAs or traditional financial assets depending on their exact nature. In particular, entities involved in any stablecoins might have AML/CFT obligations, depending on the activities these entities undertake (i.e., an activity of an FI or that of a VASP) and the design of the stablecoin (a key element being the extent to which the stablecoin arrangement is centralised or decentralised).

(e) Implementation monitoring of the June 2019 Standards

FATF completed in early July 2020 a review of the implementation of its June 2019 Standards on VAs and VASPs. FATF found that both the public and private sectors have generally made progress in implementing the revised FATF standards. FATF was advised that 35 out of 54 reporting jurisdictions have implemented the June 2019 Standards, with 32 of these regulating VASPs and three of these prohibiting the operation of VASPs, whilst the other 19 jurisdictions have not yet implemented the revised standards into national law. FATF further noted some progress in the supervision of VASPs and the implementation of AML/CFT obligations by VASPs (although generally still nascent). Progress in the development of technological solutions to enable the implementation of the “travel rule” was noted, although issues remain to be addressed by the public and private sectors for a practical implementation of the recommendations.

Considering that the VAs sector is fast-moving and technologically dynamic, FATF decided to (i) continue its enhanced monitoring of VAs and VASPs and undertook a second 12-month review of the implementation of the revised FATF standards on VAs and VASPs by June 2021, (ii) release updated Guidance on VAs and VASPs, (iii) continue to promote the understanding of AML/FT risks by publishing red flag indicators and relevant case studies, (iv) continue and enhance its engagement with the private sector, and (v) continue its programme of work to enhance international cooperation amongst VASP supervisors.

Latest discussions and developments

G-20

In its communication of June 8 and 9, 2019, the G-20 reaffirmed its commitment to applying the recently amended FATF standards to VAs and related service providers for AML/FT purposes. It is likely that essentially the G-20 will continue to rely upon FATF's position to ensure that global solutions are implemented at a broader level (through the 37 FATF Member States and the nine FATF-Style Regional Bodies). Further, in October 2019, the G-20 asked FATF to consider the AML/CFT issues relating to stablecoins, which was addressed in FATF's June 2020 report.

Bank of International Settlement

In its statement on VAs of March 2019, the Bank of International Settlement (“BIS”) recalled that VAs have exhibited a high degree of volatility and are considered an immature asset class given the lack of standardisation and constant evolution. In this respect, the BIS highlighted the various risks that VAs present for banks, including AML/CFT risks, but also liquidity, credit, market, operational, legal and reputation risks. Accordingly, the Basel Committee set out its prudential expectations related to banks’ exposures to VAs and related services that banks must at a minimum adopt (such as conducting comprehensive analyses of the risks noted above, implementing a clear and robust risk management framework that is appropriate for the risks of VA exposures and related services). According to BIS Paper No. 107 dated January 2020, however, no central bank reported any significant or wide public use of VAs for either domestic or cross-border payments, and the usage of VAs was considered either minimal or concentrated in niche groups.

UK

It is worth noting that in July 2020, the UK’s Joint Money Laundering Steering Group (“JMLSG”) updated its sectorial guidance on the AML regime applicable to UK firms active in the VA industry. The guidance provides for practical support in the implementation of AML requirements and lists the factors that may increase AML risks in the VA sector. Once approved by HM Treasury, the guidance will be used by the Financial Conduct Authority (“FCA”) in its assessment of potential breaches of AML regulations by VA firms.

Creation of specific Financial Intelligence Units

The creation of specific Financial Intelligence Units (“FIUs”) for VA-related transactions could be one of the measures to be implemented at national level that would have an impact at the international level. The cooperation between such specific FIUs would improve investigatory assistance and international cooperation in this respect (as stated in the Guidance).

Self-regulation and codes of conduct

Like Switzerland, certain jurisdictions attach great importance to self-regulation in the context of AML/CFT. Specific codes of conduct and self-regulations issued by SROs monitoring the compliance of affiliated FIs may be one of the measures that could be taken to address the ML/FT issue in relation to VAs quickly and efficiently. FIs active in the sector of cryptocurrencies, such as VA exchangers, could be specifically targeted by self-regulations adapted to their activities and providing for more clarity on their KYC and due diligence duties. Regulators and/or legislators could issue general guidelines and principles in this area, while specialised SROs could enrich them with detailed and practical recommendations until a consensus is found at the international level.

Central bank cryptocurrencies

Based on the various statements and reports on VAs issued by central banks in different jurisdictions, it appears that central banks agree that VAs such as *BTC* and *ETH* are not meant to replace fiat currency. According to the *International Monetary Fund Global Financial Stability Report* dated April 2018, the use of cryptocurrencies as a medium of exchange has been limited and their high volatility has prevented them from becoming a reliable unit of account. In this context, VAs do not appear to pose macro-critical financial stability risks at present, although if widely used, they may raise issues about, *inter alia*, ML and investor and consumer protection.

Notwithstanding the above, some 80% of central banks (such as Banque de France, Norges Bank and the Bank of England) are currently following the evolution of the developments of VAs and central bank cryptocurrencies (the “CBCCs”) closely or even contemplating

issuing their own CBCC in order to take advantage of the dematerialisation of the currency (triggering costs reductions) and to facilitate international transactions by avoiding currency exchanges issues and providing for instantaneous transfers, security and monitoring capabilities according to BIS Paper No. 107 dated January 2020.

CBCCs could be viewed as a solution to mitigate the ML/FT risks, as the transactions related thereto would necessarily go through a regulated financial intermediary subject to AML/CFT regulations. This presupposes a new generation of centralised cryptocurrencies which will not have the same level of anonymity and transferability as the current cryptocurrencies. In this respect, it is worth noting that the BIS indicated in its March 2018 report, *Central bank digital currencies*, that the issuance of CBCCs could come, in addition to more efficient and safer payments and settlement systems, with some benefits from an AML/CFT perspective. To the extent that CBCCs allow for digital records and traces, it could indeed improve the application of rules aimed at AML/CFT, as well as reduce costs of compliance. To date, we are not aware of central banks having issued their own CBCCs (with the exception of the specific case of Venezuela which has issued a state cryptocurrency backed by the country's oil and mineral reserves (i.e., the petro)).

In this context, in some part as a reaction to Facebook's Libra project and also in response to China's plans in the field of digital currencies and payments, a growing demand is forming for some form of programmable digital money which can be integrated into the existing financial system. Indeed, the potential of technology is self-evident – a national currency which is fully programmable becomes *de facto* resilient to ML/FT risks by design and would discourage non-compliant uses of such currency. However, the various risks and legitimate privacy concerns need to be addressed before such a means of payment becomes socially acceptable or desirable.

Technological solutions?

According to certain authors and actors active in the cryptocurrency field, the specific features of DL technologies and protocols could be used to mitigate the ML/FT risks in relation to VAs. KYC, beneficial owner and transactional information could be registered and verified on a dedicated DL, in the form of a global network of unalterable information (or global data repository) that would be accessible by "gatekeepers" and law enforcement. This solution, although very promising at first sight, would raise significant technical and legal issues. Among the latter, one should mention the legal requirements in terms of data protection and, as the case may be, banking secrecy. Furthermore, the access to information and its use by public authorities, such as criminal prosecution authorities, would have to be strictly regulated in order to avoid any intervention outside the applicable mutual assistance channels. In this respect, and as one of the main challenges, such a private DL would need to comply with rules enacted at an international level by the jurisdictions whose FIs would be involved in such network. It appears, therefore, that there are a certain number of obstacles as of today to using DL technologies for AML/CFT purposes, especially in the absence, at this stage, of clear guidance and standards at the international level.

As mentioned in the FATF 2015 report on VAs, other technical solutions may be available. Third-party digital identity systems, as well as new business models, could be developed to facilitate customer identification/verification, transaction monitoring and other due diligence requirements. In particular, in FATF's view, application programming interfaces ("API") that provide customer identification information, or allow FIs to set conditions

that must be satisfied before a VA transaction can be sent to the recipient, could be used to reduce the ML/FT risks associated with a VCPSS. A certain number of fintech companies have already started to develop technological AML solutions.

Conclusion

VCPSS continue to gain momentum. As adoption increases and innovation relevant to AML/CFT compliance becomes embedded in the VCPSS “genetics”, we may witness the emergence of improved existing VA protocols or entirely new VAs, built on fundamentally different underlying principles that could include built-in controls, trusted “gatekeepers”, digital identity interfaces and transaction monitoring.

Unfortunately, for as long as consistent and recognised standards and/or compliance tools are lacking, many legitimate actors in the VCPSS space will continue to be denied access to traditional banking services in a number of jurisdictions, and/or be “de-risked” by FIs. To the extent that international standard-setters, national regulators, FIs and VCPSS service providers and innovators recognise the opportunities and benefits of VCPSS globally, they should cooperate to define best practices and open, interoperable standards (as opposed to proprietary solutions), as well as training programmes for the next generation of VA “compliance officers”. Indeed, applying existing concepts and approaches tailored to an intermediated, centralised financial infrastructure simply does not work when transposed to VA ecosystems which abide by different rules and principles by design.

* * *

Endnotes

1. *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, June 2013, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>.
2. Communication from the Commission of the European Parliament and of the Council on an Action Plan for strengthening the fight against FT, Strasbourg, February 2, 2016.
3. Europol, *Drugs and the Darknet – Perspectives for Enforcement*, 2017.
4. European Central Bank, *Virtual Currency Schemes*, October 2012.
5. European Banking Authority, *Opinion on virtual currencies*, July 4, 2014.
6. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>.
7. FATF, Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, June 2020, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf>.
8. Available here: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.
9. Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of ML or FT and amending Directive 2009/101/EC, July 5, 2016 (“**MLD4**”).
10. FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014.
11. Report of the ECB on Virtual Currency Schemes, October 2012.

12. European Banking Authority, *Report with advice for the European Commission on Crypto-assets*, January 9, 2019, <https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf>.
13. The documents, some dating back to the 1970s, were created by, and taken from, Panamanian law firm and corporate service provider Mossack Fonseca, and were leaked by an anonymous source.
14. European Commission, *Explanatory Memorandum*, proposal for a Directive of the European Parliament and of the Council amending MLD4.
15. Swiss Federal Council Report on Virtual Currencies, June 25, 2014.
16. FINMA Guidance 02/2019 – Payments on the blockchain, August 26, 2019.

**Fedor Poskriakov****Tel: +41 58 450 7131 / Email: fedor.poskriakov@lenzstaehelin.com**

Fedor Poskriakov is a partner at Lenz & Staehelin in the Banking and Regulatory group in Geneva and specialises in banking, securities and finance law. He regularly advises on various regulatory, contractual and corporate matters. His practice covers banking, investment management and alternative investments, including private equity and hedge funds. He also heads the firm's Geneva office fintech practice. Highlighted as a "Next Generation Lawyer" (*The Legal 500*, 2019), Fedor Poskriakov is recognised for his "impressive expertise in the Fintech space" (*Who's Who Legal*, 2019) and "his great understating of the blockchain technology itself, combined with his concrete experience in translating this into practice" (*Chambers*, 2019).

**Maria Chiriaeva****Tel: +41 58 450 7000 / Email: maria.chiriaeva@lenzstaehelin.com**

Maria Chiriaeva is a senior associate in the Banking and Finance and the Investigations groups in Geneva and specialises in banking, securities and finance law. She regularly advises on various regulatory, contractual and corporate matters. Her practice covers banking, investment management and alternative investments. Her areas of expertise also include compliance advisory and internal investigations. Maria Chiriaeva is admitted to the Bar in Geneva. She has a Master's in economic law from the University of Geneva.

**Christophe Cavin****Tel: +41 58 450 7000 / Email: christophe.cavin@lenzstaehelin.com**

Christophe Cavin is a senior associate in the Geneva office and is a member of the Banking and Finance group and the Investigations group, respectively. His main areas of practice include banking and finance, regulatory, investigations, corporate, commercial and contractual matters. Christophe Cavin is admitted to the Bar in Geneva and New York. He has a Master's in commercial law from the University of Geneva and an LL.M. from the University of Pennsylvania Law School.

Lenz & Staehelin

Route de Chêne 30, CH-1211 Geneva 6 / Brandschenkenstrasse 24, CH-8027 Zurich, Switzerland
Tel: +41 58 450 7000 / +41 58 450 8000 / Fax: +41 58 450 7001 / +41 58 450 8001 / URL: www.lenzstaehelin.com

Decentralized Finance: Have digital assets and open blockchain networks found their “killer app”?

Lewis Cohen, Angela Angelovska-Wilson & Greg Strong
DLx Law

According to recent reports, more than \$4.16 billion in USD value¹ in the form of bitcoin, ether and other digital assets is committed to automated financial arrangements made possible through the use of open blockchain-based platforms categorized loosely as “Decentralized Finance.” A little over two months ago, this figure was only \$965 million.² It is estimated that more than the equivalent of \$25 million in value is being paid daily to users of these platforms in the form of these and other digital assets.³ This exponential growth has caused many to conclude that Decentralized Finance is not only the long-awaited “killer app” for blockchain technology but also the future of finance itself. This chapter provides an introduction to Decentralized Finance and highlights the relevant legal and regulatory issues that could accelerate or impede its growth.

What is “DeFi”?

The term “Decentralized Finance” (often referred to simply as “**DeFi**”) is broadly used to refer to a new paradigm involving financial products built on open (permissionless) blockchain-based networks, such as Ethereum, and generally utilizing digital assets, such as bitcoin and ether.⁴ DeFi platforms are generally promoted as being “decentralized” or at least “disintermediated,” although what these terms mean in this context is subject to debate. What can be said is that almost all DeFi products and services are *automated*, meaning that once a transaction is initiated, computer code stored on the relevant blockchain network (generally known as “**smart contracts**”) will carry out the transaction transparently and deterministically. They are also generally *non-custodial*, meaning that no centralized party is holding assets on behalf of any user of the relevant platform or other party.

Interoperable, programmable, and composable,⁵ the networks built using open blockchain protocols have the potential to serve as the foundation for decentralized alternatives to nearly every traditional financial service, including retail payments, swaps and derivatives transactions, insurance, asset trading, exchange and management, deposit and savings accounts, lending, and investing. DeFi is the manifestation of this concept, although only time will tell if it will be able to fulfill its full potential of enabling a parallel global decentralized financial ecosystem.

Permissionless blockchains with sophisticated, Turing-complete scripting and programming languages like “Solidity,” the coding language for Ethereum, allow any developer (or group of developers) anywhere in the world to create complex functions that execute automatically on-chain when a certain set of conditions are met, establishing a new, open environment that can mimic many aspects of existing financial services. These functions, also known as decentralized applications (or “**dApps**”), utilize blockchain-based protocols that can operate with little to no human intervention, removing the need for a centralized

intermediary to monitor and verify transactions (as well as removing the benefits such centralized parties can provide). Often, a centralized entity is not even needed to grant users access to the relevant dApp, because both the dApps and the decentralized network protocols⁶ on which they operate are completely open for all to use. Typically, anyone from the general public may inspect the underlying computer code governing these protocols, give instructions to a particular network to create transactions, and participate in a particular network's transaction validation and consensus process.⁷

As a result of this open architecture, DeFi presents both unique risks and unique risk-reducing benefits when compared with traditional intermediated financial services. For example, the Financial Stability Board (“FSB”) found that DeFi has the potential to reduce public reliance on existing financial services providers for channeling funding into lending, which could likewise reduce those providers' solvency and liquidity risks.⁸ The financial stability implications of any particular DeFi platform might depend on how much it decentralizes an existing financial market and the prevalence of its application in the financial services industry more broadly.⁹ In addition to overall systemic financial stability, DeFi may also have benefits (or raise concerns) in a variety of other areas, such as consumer privacy and protection, financial market reliability, resilience and efficiency, and financial crime prevention.

Twelve years after the pseudonymous Satoshi Nakamoto published the Bitcoin whitepaper, once obscure blockchain-based cryptocurrencies and other digital assets are now familiar to many. The recent growth in the creation and development of new types of digital assets that exist on blockchain-based networks, like digital assets whose value is pegged in some manner or another to that of an existing fiat currency (known as “stablecoins”), tokens that facilitate the governance of an open blockchain protocol (discussed below), and the potential development of central bank-issued digital currencies (“CBDCs”) utilizing distributed ledger technology, has put blockchain technology in the spotlight. Although Bitcoin and many other early blockchain networks that followed it rely on energy-intensive computational algorithms (known as Proof of Work, or “PoW”) for network security, subsequent mechanisms associated with validating transactions and achieving consensus like Proof of Stake (“PoS”) seek to enhance efficiency, reduce transaction costs and improve scalability, and mitigate the risks associated with the use of digital assets and dApps. The DeFi ecosystem currently exists primarily on the Ethereum network and includes Ethereum-based platforms like “MakerDAO,”¹⁰ “0x,”¹¹ and “Compound,”¹² as well as emerging protocols like Aave,¹³ Balancer,¹⁴ and dYdX,¹⁵ although new platforms and protocols are coming online rapidly.

This remarkable level of growth and development has resulted in the creation of a seemingly unlimited number of DeFi use cases, like collateralized lending, insurance, primary and secondary market asset exchange, and new money markets. DeFi proponents have found the ability to compose transactions that can involve steps utilizing multiple DeFi platforms and use cases to programmatically achieve a particular objective without the need to create relationships with traditional intermediaries like broker-dealers, lenders or exchanges, to be a powerful benefit. What follows is a discussion of these various DeFi system functions and services and their potential legal implications.

DeFi protocols

As described above, DeFi protocols have a wide variety of use cases. We explore at a high level a few of the most utilized protocols and use cases below. These include lending, borrowing, peer-to-peer (“P2P”) exchange, and combinations of these activities designed to

create yield on non-interest-bearing digital assets. We also examine the governance of these protocols and identify legal issues raised by the operation and governance of these protocols. However, the DeFi landscape continues to evolve rapidly and protocols that are popular today may be out of favor and supplanted by others by the time this chapter is printed.

Background

Before we look at specific protocols, a word about the open-source nature of public blockchains, decentralized autonomous organizations (“**DAOs**”), and dApps is necessary to set the stage for this discussion. Most DeFi platforms are explicitly or implicitly established to accomplish some sort of business purpose (e.g., facilitating P2P lending transactions) and are generally intended, presently or at least at some point in the future, to operate without a central point of command and control, and thus can be considered “DAOs.” The concept of decentralized business organizations was postulated by academicians as early as the 1930s,¹⁶ and commented upon by business writers more recently¹⁷ but made possible as a practical matter only with the advent of blockchain technology. Alternatively, the idea of a network application that operates autonomously was developed directly in response to the availability of the Ethereum network.

It is of critical importance to DeFi protocols that they operate on public blockchains with open-source code. Typically, the developer of a DeFi protocol that is intended to be decentralized will attempt to turn governance and responsibility for the computer code underlying the protocol over to the community of users of the protocol. One way this can be accomplished is through the distribution of a digital asset that provides the owner of the asset with the right to participate in governance decisions with respect to the relevant protocol (generally referred to as “**governance tokens**”). Members of the user community (whether through the use of governance tokens or otherwise) may be able to propose updates to the platform codebase, vote on whether these updates should be adopted, and/or make other decisions about the operation of the protocol. Ideally, users of the decentralized protocol will have the technical ability to understand the underlying code, what it is designed to accomplish, and whether the code as written meets the intended design goals in order to effectively make these decisions – although there is an obvious tension between this ideal and the ability of the protocol to sustain very high levels of user growth. In the case of some platforms, voting on governance matters can be delegated to others the token holder deems more technologically sophisticated or generally better suited to make these decisions.¹⁸

Regardless, due to the absence of controlling intermediary, users of a decentralized protocol who want to protect their interests will need to have a fairly high degree of technological competence in order to evaluate the risks that they and other users are taking by engaging in transactions utilizing the relevant protocol. Again, ideally, users should be familiar with the codebase underpinning the protocol and have the technical competency to identify vulnerabilities and potential exploits (or, at a minimum, to evaluate the relevance and importance of vulnerabilities identified by others). This includes understanding whether any particular party retains access control over the smart contracts or has independent authority to make changes to the code or the operation of the protocol. In addition, because DeFi protocols are open source and available to anyone, sophisticated users with malicious intent can also access and analyze the code to identify vulnerabilities to exploit for their own benefit.

In more formal terms, a “DAO” is a complex smart contract structure that can automate transactional protocols with little need for additional programming. DAOs are generally built on an advanced, Turing-complete blockchain such as Ethereum that relies on algorithmic structures and may also use artificial intelligence tools to manage group activity. Turing

completeness describes a computational ruleset that—like most contemporary computer programming languages—can recognize or complete other data-manipulation rulesets.¹⁹ The blockchain on which the DAO is built employs timestamping and a distributed database to simplify transactions by removing the need for a trusted third party to facilitate interactions among counterparties. Decentralized trusted timestamping involves a set of secure blockchain protocols that track creation and modification times for a smart contract. Although not strictly “immutable,” most DAOs and other decentralized networks employ various apparatuses to deter tampering and exploitive attacks, depending on the mechanism used to secure the underlying blockchain network.

A dApp is a computer application that has backend code that runs on a decentralized P2P network, such as a blockchain network, and which is, or is intended to become, decentralized (*i.e.*, not controlled by a centralized party). By contrast, traditional computer applications have backend code that runs on centralized servers controlled by a known and identified party. The frontend code and user interfaces of a dApp will call to the decentralized backend code to allow users to provide instructions to the smart contracts comprising the dApp.

A “stablecoin” is a type of digital asset designed to serve as a better store of value relative to a designated fiat currency when compared to typical cryptocurrencies and other digital assets. Cryptocurrencies typically exist on a blockchain-based decentralized network and are often subject to high volatility since their value is usually based solely on market demand and speculation. A stablecoin can be issued and administered on either a decentralized network or a centralized, closed-loop system, and uses a mechanism to ensure at least a somewhat stable value.²⁰ A stablecoin can be intended for use as payment in exchange for other digital assets or as an alternative to fiat currency.

Stablecoins are important for DeFi because they provide a digital onramp for users that is stable in value relative to a widely used benchmark, like the U.S. dollar. They can serve as a bridge from the traditional financial system to the digital financial world, particularly when they are backed by a traditional financial asset. As stablecoins become more widely adopted, we can expect that digital finance and DeFi will grow.²¹

One final observation of critical importance to DeFi: most blockchain-based digital assets do not bear interest or provide holders with the right to dividends or equivalent distributions that are denominated in a fiat currency. As a result, unless a digital asset is being held for purposes of its primary utility (*e.g.*, in the case of ETH, using the ETH tokens to pay the “gas” charge to launch smart contracts on the Ethereum network), the only financial reason to own the asset is for anticipated price appreciation. Accordingly, to own a digital asset means foregoing any potential for income from the value represented by that asset until the asset is sold. As a result, many owners of digital assets look for ways to earn income from those digital assets they intend to hold on a long-term basis – DeFi platforms provide exactly that opportunity. As more people become interested in, and invest in, digital assets, it is anticipated that demand for ever more creative DeFi solutions will only increase.

Specific protocols

MakerDAO is an example of an open-source “DAO” project utilizing the Ethereum blockchain that allows users to borrow, lend, and exchange digital assets, and was one of the first DeFi platforms to gain significant adoption. Users of the MakerDAO platform can generate and borrow a stablecoin called “**Dai**,” the market price of which is algorithmically pegged to the U.S. dollar, by depositing eligible digital assets into a “**Vault**.”²² Each Vault is responsible for paying a stability fee,²³ which is variable and accrues over time, on the Dai balance generated by that Vault. Stability fees may be paid in Dai at any time and

a Vault owner must make sure that the Collateralization Ratio in the Vault never drops below the applicable Liquidation Ratio. The Collateralization Ratio is the ratio of the value of the collateral in a Vault to the value of the Dai generated by the Vault.²⁴ All Vaults must be overcollateralized. The Liquidation Ratio is a minimum Collateralization Ratio for a given type of Vault that is set in accordance with MakerDAO governance.²⁵ If the Collateralization Ratio of a Vault falls below the Liquidation Ratio applicable to that Vault, the collateral assets in the Vault may be liquidated in exchange for Dai in order to recover the Dai generated by the Vault.²⁶

In addition to depositing collateral to generate Dai stablecoins, MakerDAO users can also deposit Dai to earn additional Dai at the Dai Savings Rate (“**DSR**”) and can engage in the P2P exchange of assets using a decentralized exchange on the MakerDAO platform.²⁷

Other DeFi applications, like 0x, contain built-in protocols to facilitate the P2P exchange of ERC-20 tokens²⁸ on the Ethereum blockchain through the use of additional services provided by “**relayers**,” providing an open order book infrastructure on which DAOs and other dApps can be built.²⁹ This allows for the creation of decentralized exchanges in both primary and secondary markets, which can be seamlessly integrated with other blockchain-based networks. A dApp built on the 0x protocol can access existing public liquidity pools or create its own liquidity pool, charging transaction fees on the resulting volume. This enables market creation for digital assets where markets might not previously exist. As more traditional financial assets become tokenized or digitized, 0x essentially permits developers to combine different public blockchains to create new, more efficient and transparent financial architecture. Critically, the 0x protocol itself is oblivious as to whether a given regulator in a given jurisdiction would consider the ERC-20 token a “security” or other type of regulated instrument. Management of this risk must occur outside of the protocol.³⁰

Compound is another, more recent, DeFi application developed by Compound Labs, Inc. Compound uses Ethereum-based protocols on which DAOs or dApps can be built to establish new money markets.³¹ Asset suppliers and borrowers within these money markets³² may interact directly with the Compound protocol to earn or pay a floating interest rate. Compound helps to lower money market transaction costs by removing the need for counterparties to negotiate over terms. It supplies a transparent, public ledger that includes a complete transaction record and a historical record of interest rates. Persons already holding digital assets like BTC and ETH can use these assets as collateral in a Compound money market to generate additional returns.³³

Compound has pursued a strategy of progressive decentralization that is intended to ultimately culminate in the user community governing the Compound protocol.³⁴ The transition from administrator governance over the protocol to user community governance is being accomplished through the allocation of a governance token called “**COMP**.” COMP holders are permitted to suggest, debate and implement changes to the Compound protocol. These functions were previously performed by the administrator of the Compound protocol. COMP holders may also delegate voting rights to an Ethereum address of their choice. According to Compound, COMP tokens have been allocated as follows:

- 2,396,307 COMP have been distributed to shareholders of Compound Labs, Inc.;
- 2,226,037 COMP are allocated to Compound Labs’ founders and team, and subject to four-year vesting;
- 372,707 COMP are allocated to future team members;
- 4,229,949 COMP are reserved for users of the Compound protocol;
- 775,000 COMP are reserved for the community to advance governance through other means—which will be announced at a future date; and
- 0 COMP will be sold to, or retained by, Compound Labs, Inc. itself.³⁵

The 4,229,949 COMP reserved for the users of the protocol are being allocated daily. Both borrowers and lenders using the Compound protocol can receive a portion of the 2,880 COMP tokens allocated each day for providing liquidity to the protocol. Incentivizing participation in a DeFi protocol to enhance liquidity on the protocol through the allocation of rewards, in the form of a token or otherwise, has come to be known as “**liquidity mining.**” COMP tokens, as of this writing, were valued at \$155.52 each. The value of COMP has created a situation in which rational participants in the system, in certain circumstances, can justify paying to borrow an asset they have also lent, all through the platform, in order to earn COMP from liquidity mining. Although the ostensible purpose of COMP is to allow holders to participate in governance of the Compound protocol, it also has developed significant value in secondary markets, perhaps due to a perception that COMP holders will ultimately benefit financially from the success of the Compound platform. Following the success of COMP, similar governance tokens are being distributed by other DeFi platforms to incentivize user participation and enhance liquidity.

Liquidity mining is related to another DeFi concept called “**yield farming.**” Yield farming refers to utilizing digital assets, often on one or more DeFi platforms, in order to generate a return on those assets. Liquidity mining is one way to engage in yield farming.

Due to the lack of a centralized responsible entity, it is critical for users of DeFi platforms, including users seeking to create a return on non-interest-bearing digital assets through yield farming, to understand how the platforms are governed and the process for changes to the relevant protocols. For example, with respect to MakerDAO, if the stability fee or the Liquidation Ratio applicable to a particular Vault is changed in accordance with the Maker governance system, it can have a significant financial impact on Vault owners and borrowers.

The MakerDAO governance system was tested on “Black Thursday,” a period of time between March 12 and 13, 2020 in which the prices of many digital assets declined by approximately 50% (along with huge declines in the traditional equity markets). The sharp price declines in ETH and other digital assets caused the Liquidation Ratios in many Vaults to be breached, which triggered automated collateral liquidations via auction according to the MakerDAO governance scheme. Network congestion on Ethereum and associated high “gas” prices³⁶ during this time made it difficult for users to either post additional collateral to their Vault(s) or return Dai to their Vault(s) to unlock collateral. The decline in digital asset prices, coupled with an inability of users to post additional collateral or unlock collateral due to network congestion and high gas prices, resulted in 1,200 Vaults being automatically liquidated and their contents auctioned. In some cases, the winning bid for collateral being liquidated was zero, meaning the successful bidder obtained collateral at auction for zero Dai. According to one report, more than \$8 million in collateral was liquidated for zero Dai during this period.³⁷

The “Black Thursday” event was an extreme situation, but the MakerDAO zero-bid automated liquidations highlight some of the risks of locking value in new and often not fully tested protocols. In addition, recent reports examining the transaction activity on the Ethereum blockchain on Black Thursday suggest that the network congestion and high gas prices that contributed to the situation were deliberately engineered by bots operated by actors looking to benefit from the chaos.³⁸

The impact of Black Thursday price declines on MakerDAO can be analogized to the stock market crash of October 19, 1987, referred to as “Black Monday.” On Black Monday, the equity markets lost more than 22% of value in a single day. Shortly thereafter, President Reagan appointed a task force to determine the causes of the crash and to make recommendations to prevent a similar crash in the future.³⁹ The task force attributed the

Black Monday crash, at least in part, to computer-driven automated programmatic trading by institutions that was ignited by a more modest initial decline in prices.⁴⁰ Accordingly, one of the recommendations in the Brady Commission Report designed to contain mass selling, whether automated or otherwise, involves the concept of “circuit breakers.” In the case of the equity markets, circuit breakers are trading halts triggered by defined percentage drops in the S&P 500 Index.⁴¹ Halts can occur three times in a given day, with the first two suspending trading for 15 minutes and the third suspending trading for the day. Circuit breakers are designed to provide a time-out to market participants to allow them to evaluate what is happening, assess liquidity and order imbalances, and prevent panic-selling. On Black Thursday of this year, circuit breakers in the equity markets were triggered and the market subsequently stabilized.

It took the dire events of 1987’s Black Monday to implement “circuit breakers” in the formally organized equity markets. The DeFi space has already reflected on the events of Black Thursday 2020, and new mechanisms will no doubt be proposed to address such a situation in the future. The ability to implement workable and effective proposals to address the potentially hazardous consequences on DeFi users of purely automated collateral liquidation will be a serious test of whether decentralized governance can be effective and whether multiple decentralized protocols, each potentially exposed to the risks of the other, can coordinate to establish circuit breakers, collectively monitor ephemeral mempool data for unconfirmed transactions posing risks to instruction execution, or take other collective steps in order to prevent future Black Thursdays.

Proof of stake networks and staking as a service

Digital assets that exist on decentralized blockchain-based networks require a way for participants to verify on-network transactions absent a designated intermediary while maintaining the security of the network.⁴² PoS is the most common alternative⁴³ to the widely known PoW system—which is employed by Bitcoin and other major digital asset protocols. Both PoS and PoW systems include protocols by which nodes reach agreement as to whether a given transaction is valid under the rules of the protocol and should be added to the ledger. Protocols typically create groups (or “**blocks**”) of transactions that can only be added to the common ledger when validated by a sufficient percentage of all nodes in the network. Both PoS- and PoW-based open blockchain networks use open-source software which can be freely downloaded and run by anyone with the necessary hardware and technical capability. The ledger of transactions on open blockchain networks can also be viewed by anyone with a computer and Internet connection.

Proof of stake networks

PoS networks rely on minters (or “**validators**”) to confirm the accuracy of each block added to the network ledger. In order to secure a PoS network, validators are required to “**stake**”⁴⁴ tokens to add validated transactions to a block and to mint new blocks to the chain. The PoS mechanism is a Sybil-resistance tool⁴⁵ that incentivizes validators to confirm transactions that conform to the rules of the protocol by slashing the staked tokens of a validator that confirms an invalid transaction. Validators utilizing their digital assets to participate in PoS are securing the relevant network and receive staking rewards for doing so.

A PoS network might establish a staking inflation rate from five to 50% on an annualized basis,⁴⁶ which serves to incentivize digital asset holders to stake their assets and participate in securing the network. A validator collects newly minted native digital assets based on these

staking inflation rates and sometimes other transaction fees for the blocks she validates. These **“Rewards”** encourage validators to participate in the network and help to secure and decentralize it. A validator’s staked assets give her skin in the game: she risks losing all or some of her bonded digital assets or forfeits Rewards for node failures, mistakes, or instances of fraud. These forfeitures and penalties are called **“Slashing.”** Holders of digital assets native to a PoS network that do not participate in staking will lose value over time because they will not accrue Rewards.

Staking for returns

To participate as a validator on a PoS network, a native digital asset holder can act as principal to stake her own digital assets in a bonded wallet, validating transactions and earning Rewards on her own behalf. The participant will encounter several complex security and technical issues, however, in establishing and maintaining a staking operation and running a network node. Plus, the participant is exposed to Slashing risks if she does not properly manage the validation process.

Many PoS networks recognize that the requirements and risks involved in staking as principal might disincentivize digital asset holders from participating in validation, and therefore allow firms to offer holders staking as a service (**“StaaS”**). StaaS allows a digital asset holder to earn staking Rewards without having to deal directly with the validation process.

Some PoS networks allow a digital asset holder to transfer or **“Delegate”** her validation rights to a StaaS provider while retaining custody of her staked assets (**“Delegation”**). These Delegated Proof of Stake (**“DPoS”**) networks allow a holder to essentially self-custody and stake her own digital assets but contract with a StaaS provider to validate blocks of transactions and earn Rewards on the holder’s behalf. Some other PoS networks, however, require the participating holder to transfer custody of her digital assets to the StaaS provider to stake the assets, validate blocks, and earn Rewards on the holder’s behalf.⁴⁷

A StaaS provider essentially acts as a third-party validator. Like every validator, the StaaS provider can choose whether to include certain transactions in a block, but cannot change transaction details like senders, recipients, or the asset balances involved. A StaaS provider is disincentivized from abusing its power to add blocks to the PoS network’s ledger due to Slashing risks, which allow for system self-governance. A StaaS provider facilitates access to the computer hardware and software necessary for operating a node, validating on-chain transactions, and earning Rewards, which might be too complicated or costly for a digital asset holder to access on its own.⁴⁸ The StaaS provider will typically charge a set service fee to its customer holder equal to a percentage of the Rewards earned on behalf of the holder.

Although those who already hold digital assets that comprise part of a PoS network may choose to stake those assets directly or through a StaaS provider, the presence of a robust market of StaaS providers means that others interested in earning a return in the digital asset space may choose to acquire digital assets expressly for the purpose of earning Rewards. Thus, staking itself can be thought of not only as a means for providing network security but also as an alternative type of DeFi.

Regulatory issues in DeFi

The blockchain protocols on which DeFi platforms are built are open, immutable (to a large extent), and transparent, and potentially allow regulators to observe platform activity as it occurs in real time. In theory, at least, compliance with various regulatory requirements can be built into the protocols or the platforms running on those protocols. However, there are

some clear practical and operational limits to this, given that DeFi platforms operate across borders and users may hail from nearly every jurisdiction, making consistent, automated, regulatory compliance a virtually unattainable goal (not to mention the challenges of decentralized platforms responding to the rapid changes in regulatory requirements going on in many jurisdictions). In addition, the absence of a traditional, central intermediary for any given DeFi platform raises many new regulatory considerations and different risks, and involves increased technical complexity. All of these factors combine to make it difficult to predict how existing regulatory structures will be applied to DeFi platforms. Below, we offer some thoughts about the legal and regulatory issues relevant to the DeFi use cases we focused on in the “DeFi protocols” section above: borrowing and lending; decentralized asset exchange; and combinations of these activities.⁴⁹

Decentralization

Before delving into the specifics, the question of what it means to be “decentralized” is an important starting point for this analysis. Decentralization can be relevant in a variety of contexts. It can refer to the manner in which transactions on a particular blockchain network are validated. It can also refer to the manner in which blockchain protocols are governed and how decisions regarding updates and changes to a given protocol are made. It can refer to the breadth of wallet addresses holding a token native to a particular blockchain protocol or a token issued by a dApp sponsor.⁵⁰

All of this begs the question: what does the “decentralized” in DeFi mean? As set out above, decentralization can refer to many different aspects of a protocol and can mean different things to different people. In the context of legal and regulatory analyses, the most important issue will be whether there is an identifiable actor (or group of actors) whose relationship with the relevant platform appropriately results in those actor(s) having regulatory responsibility. The key question in determining this will be whether a dApp or protocol that labels itself as “decentralized” is able to operate, and in fact does operate, without the implicit or explicit reliance on, or control by, an identifiable responsible party and without a single identifiable party (or limited number of identifiable parties) that are benefiting financially from the operation of the protocol in a disproportionate way.

From a securities law perspective, the concept of decentralization is relevant to the investment contract analysis in the *Howey* test, particularly with respect to evaluating the *Howey* factor related to the “essential managerial efforts of others.”⁵¹ According to the staff of the U.S. Securities and Exchange Commission (“SEC”), as laid out in their Token Framework, the key question for purposes of determining whether a token seller has created an “investment contract” is whether the seller is an “active participant” that purchasers of a digital asset rely upon to drive the value of the asset.⁵² In this context, “control” is a key element. For instance, does an individual, entity, or group of individuals or entities effectively control a DeFi platform? Do they hold a large portion of the governance tokens for the platform? Are they disproportionately driving the marketing and promotion of the platform to the general public? Do they control the smart contracts that make up the protocol? Can they make unilateral changes to the protocol or the relevant smart contracts? Are they the only ones who can effectively propose changes to the protocol? Do they receive a significant financial benefit from participating in the operation of the platform?

All of these are questions that regulators, and not just securities regulators, are likely to ask in determining whether there is a party that should bear regulatory responsibility for the activities facilitated by DeFi protocols. Part of this analysis will also be a pragmatic one: assuming something goes wrong with or on the platform, would regulators in a given

country be able to identify (much less obtain jurisdiction over) one or more actors who are theoretically responsible for whatever happened?

The application of the U.S. federal securities laws by the SEC to a decentralized exchange provides an instructive example.⁵³ EtherDelta was designed as a protocol for the P2P exchange of digital tokens and was billed as “decentralized.” The SEC entered into a consent order with Zachary Coburn, an individual and the founder of EtherDelta, to resolve an investigation into violations of the federal securities laws.⁵⁴ The order alleged that at least some of the tokens traded on EtherDelta were unregistered securities and that Coburn had caused the EtherDelta “trading system” to violate certain provisions of the Exchange Act, on the basis that he: (i) founded EtherDelta; (ii) coded and deployed the EtherDelta smart contract; (iii) had exclusive control over the EtherDelta smart contract (including the ability to change the fees charged for exchanges); and (iv) served as a spokesperson for EtherDelta on Twitter and Reddit.⁵⁵ Here, the SEC looked past the label “decentralized exchange” to identify a party with the requisite control over the protocol to have regulatory responsibility.⁵⁶ We think most U.S. financial regulators will perform a similar analysis with respect to DeFi platforms to identify actors they believe should bear responsibility for regulatory compliance by the platform.

Regulation of institutions or activities

Following the 2008 Global Financial Crisis, the U.S. focused on institution-based regulation and oversight of both banks and non-bank financial firms with the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the “**Dodd-Frank Act**”). The institution-based approach to regulation is focused on risk at the firm level and may not capture risky financial activities occurring outside of regulated institutions. Institution-based regulation can also encourage pushing riskier activities out of regulated firms and into firms that are not regulated.

Because regulated entities are not part of the DeFi landscape, the institution-based approach to regulation may miss potentially risky financial activities that would otherwise be subject to regulatory oversight had they occurred within a regulated entity. This may continue until the amount of value locked in DeFi platforms is sufficient to cause regulators to take notice, or there is a major loss event that draws their attention. As more financial activities move towards decentralization and the financial system grows ever more globally interconnected, new regulatory approaches will likely need to be developed. Despite efforts by global financial regulatory bodies to harmonize law and regulation among developed and developing countries, the approaches of domestic regulators still vary widely. The Financial Stability Oversight Council—which was established by the Dodd-Frank Act to coordinate regulatory approaches among U.S. domestic financial regulators—made a major shift in its 2019 guidelines⁵⁷ to emphasize an *activity-based approach* to regulation for non-banks after its own attempts to implement enhanced, institution-based regulations for non-banks it deemed systemically important. Going forward, and in consideration of the unique risks posed by DeFi, the activity-based approach will be critical to developing adequate oversight in the jurisdictions where DeFi activities reach investors or consumers.

Persons or entities that administer or facilitate the use of DeFi services must consider how their activities might be regulated in each jurisdiction in which the relevant platform experiences significant activity, even where the law in that jurisdiction is unclear. For example, the U.S. Commodity Futures Trading Commission (“**CFTC**”)’s LabCFTC published a primer on smart contracts reiterating the common law contracts principle that—to the extent a [smart] contract violates any law or regulation—it likely will not be

binding or enforceable.⁵⁸ To understand regulatory implications in DeFi, both regulators and industry participants must understand a decentralized network's rules, how the network is governed, and what activities any dApps built thereon can facilitate. Once the operation and activities of a DeFi platform are well understood, existing law can be applied to those specific circumstances as appropriate.⁵⁹

Lending

A primary regulatory consideration in DeFi concerns lending. Internet-based P2P lending first appeared for personal loans in the aftermath of the 2008 Financial Crisis, and its development since then provides some parallel considerations for DeFi lending platforms. Over the last decade, Internet-based lending has expanded to include small business lending and mortgage lending. P2P lending (also known as “**marketplace lending**”) was initially seen as a gray area for facilitating small personal loans directly from investors with no licensed intermediary. The reality is that, in the U.S., lending is regulated pursuant to both state and federal laws. This has led many P2P lending platforms, like Lending Club, to subscribe to the bank-partnership model. Under this model, the lending platform will typically operate lending programs for a partnering bank, which will originate loans taking advantage of federal preemption under the National Banking Act and then sell those loans back to the platform to subsequently securitize or otherwise sell to investors. This process involves compliance with lending laws through bank partnerships and compliance with securities laws through shelf registrations in order to facilitate these loans. One of the reasons P2P lending platforms have pursued partnerships with banks is that compliance with the patchwork of U.S. state lending laws, necessary to offer nationwide products, can be challenging and expensive. At the end of the day, these loans are not simply “P2P” as originally conceived and the platforms facilitating these loans play a significant central role. So, when is a state lending license needed for P2P loans effected programmatically by computer code? First, state banking regulators could pursue a similar approach to that taken by the SEC in EtherDelta in which Zachary Coburn was held responsible for the decentralized trading platform he created, controlled, and profited from. However, this approach entails finding an individual (or group of individuals, investors and/or businesses) who can be credibly held accountable in the same manner as Mr. Coburn was with EtherDelta. Given the prevalent use of governance tokens to disperse responsibility for protocol maintenance and the lessons learned by the DeFi community from enforcement actions against EtherDelta and others, that may be easier said than done.

If an enforcement action is commenced (perhaps due to consumer complaints), to the extent responsible actors that directed and/or benefited from lending activities that would otherwise have been subject to regulation can be identified (and properly served), they will likely be held responsible for deemed non-compliance by the platform. It is important to note that the scope of many state lending as well as consumer protection laws is broad. In Delaware, for example, a person transacting the business of lending money must be licensed.⁶⁰ “Person” is defined broadly to include any group or combination of individuals however organized.⁶¹ In addition to the broad definition of person, any member or agent of a group or combination of persons may be proceeded against as a principal for failure of the group or combination to obtain a license as required.⁶² So, although it may be difficult to identify the appropriate license holder with respect to a decentralized lending platform, state lending statutes may be broad enough to cover a wide variety of groups of participants, even when not formally organized.

The second key aspect of this analysis relates to the definition of “money” in a given state. The non-bank lending licensure requirement in Delaware, for example, applies to transacting the business of lending *money*.⁶³ The question, then, is whether loans denominated in digital assets such as ETH or Dai constitute “money” as that term is used in the statute. The term “money” is not defined in Delaware, but whether certain digital assets fall within the definition of money for purposes of lending and money transmission has been clarified in other states as discussed below. To the extent a state does not treat virtual currency or other digital assets as money, such as in Pennsylvania,⁶⁴ lending and money transmission activities will likely not be deemed to be regulated by the banking regulator. In other states, such as Washington state,⁶⁵ the opposite is likely the case.

Loans, including P2P loans, may be void *ab initio* or rendered voidable if not facilitated by an entity with a valid lending license.⁶⁶ Given the breadth of potential application of state lending laws, developers of and groups that together control decentralized lending platforms should consider what, if any, regulatory obligations they may be deemed to have and how they would respond upon an inquiry from a state or federal banking regulator.

Money transmission

DeFi platforms whose activities involve convertible virtual currency (“CVC”) should consider whether compliance with state and federal laws and regulations applicable to money services businesses and money transmitters is necessary. The U.S. Treasury’s Financial Crimes Enforcement Network (“FinCEN”) released relevant guidance in May of 2019 with respect to the potential obligations of DeFi platforms.⁶⁷ In the 2019 Guidance, FinCEN indicated that the “determination of (a) whether the specific person meets the definition of a particular type of financial institution and (b) what regulatory obligations are associated with the specific activities performed within the business model” is dependent on key facts and circumstances.⁶⁸ The “label [adopted by a given business model], however, will not determine the regulatory application,” making clear that FinCEN will make a substantive inquiry to determine the regulatory responsibility of any given entity.⁶⁹

FinCEN’s regulations apply to money services businesses, including money transmitters. A money services business is defined as “a person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States,” operating directly, or through an agent, agency, branch, or office, who functions as, among other things, a “money transmitter.”⁷⁰ The term “person” is defined as “an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities.”⁷¹ This definition is similarly broad to the definition of person in the state lending laws and includes groups that are not formally organized.

“The term “money transmission services” is defined to mean *the acceptance of* currency, funds, or *other value that substitutes for currency* from one person *and the transmission of* currency, funds, or *other value that substitutes for currency* to another location or person by any means.”⁷² CVC⁷³ is “other value that substitutes for currency.”⁷⁴

FinCEN Guidance refers to three categories of participants with respect to the CVC ecosystem: “Users;” “Exchangers;” and “Administrators.”⁷⁵ An Exchanger is a person engaged in the business of exchanging virtual currency for “real currency, funds, or other virtual currency.”⁷⁶ An Administrator is a person engaged in the business of issuing virtual currency and has the authority to redeem it.⁷⁷ While a User is not a money transmitter, both

an Exchanger and an Administrator are considered money transmitters if they either accept and transmit or buy or sell virtual currency and thus must register as money transmitters and comply with FinCEN's regulatory framework.⁷⁸

The 2019 Guidance assesses common business models that engage with CVC and sets forth the circumstances in which a business model involves Exchanger or Administrator activity that would subject operator(s) of businesses adopting that model to compliance with FinCEN regulations.⁷⁹ The Guidance specifically addresses dApps, indicating that “when DApps perform money transmission, the definition of money transmitter will apply to the DApp, the owners/operators of the DApp, or both,” regardless of whether there is an identifiable Administrator.⁸⁰ If there is a person or group that is collecting a fee from Users running the dApp software and it engages in money transmission, *any* ultimate beneficiary of those fees that can be identified and prosecuted by FinCEN will likely be deemed to have regulatory responsibility. FinCEN further noted that the same regulatory interpretation that applies to mechanical agencies, such as CVC kiosks, will apply to dApps.⁸¹ Accordingly, as far as FinCEN is concerned, those it considers owners or operators of DeFi platforms that accept and transmit CVC will be deemed money services businesses. It is also important to note that in addition to the federal regime, those who effectively control, or who economically benefit from, DeFi platforms that accept and transmit CVC in the U.S., must also consider the intricate web of state money transmission laws with which the platform might have to comply. Heightened scrutiny of DeFi platforms that provide services of this nature without conducting the know-your-customer checks that would be required to comply with the BSA, FinCEN as well as state money transmission regulations, should be expected.

Securities laws

Any DeFi platform must consider whether each individual digital asset it issues or otherwise deals in might be considered a “security” under U.S. law. If so, securities laws will apply. The definition of security in the federal securities laws includes an enumerated list of instruments. A digital asset or a transaction involving a digital asset may be any one of the instruments included in that definition.

An “investment contract” is one of the enumerated instruments in the definition of a security. Whether a transaction involving a digital asset (or the digital asset itself) is deemed a security will usually be determined by application of the *Howey* test.⁸² An investment contract under *Howey* involves (1) an investment of money, (2) in a common enterprise, (3) with the expectation of investor profit, (4) derived solely from the efforts of others.⁸³ If all four elements of the *Howey* test are satisfied, then a scheme to sell an asset will be deemed an investment contract and a security subject to compliance with the securities laws. Under such circumstances, the SEC may also consider the specific digital asset a “security” as well. Such a conclusion would have significant implications for the person deemed to be the seller of a security as well as anyone that facilitates secondary trading in the security (as we saw with the Coburn Order and as described below).

Stock is also an enumerated instrument within the definition of the term “security.” “Stock” is composed of a bundle of rights enjoyed by the holder or owner and may include the following traditional characteristics: an ownership interest in the issuing entity; voting rights in proportion to the shares owned; the right to receive dividends in apportionment of profits; negotiability; the ability to be pledged or hypothecated; and the ability to appreciate in value.⁸⁴

Governance tokens for DeFi platforms have exploded in popularity recently. These tokens are typically issued by DeFi platforms to incentivize use of the platform and drive participation. They typically provide voting rights to transition the platform to decentralized

governance by the token holders. They also appreciate in value as the popularity of the platform increases, ostensibly because the holders of the tokens will exert control over the platform and collectively benefit from the operation of the platform. They typically can be negotiated and pledged. Whether governance tokens constitute “stock” (or another type of “security”) is for the regulators to determine, but DeFi proponents must acknowledge that there is an argument to be made that these tokens generally appear to convey constructive ownership and voting rights to their owner.

A security sold in the U.S. must either be registered with the SEC or exempt from registration; secondary exchanges of securities must be conducted on exchanges regulated by the SEC or occur in exempt transactions; and distributions of securities may be made only by broker-dealers properly registered with the Financial Industry Regulatory Authority (“**FINRA**”) or in exempt transactions. Although a trading venue that allows clients to trade digital assets deemed to be “securities” must be registered as an exchange with the SEC under the Securities Exchange Act, some venues that use permissioned blockchains for trading tokenized securities, like OpenFinance and tZERO, are exempt by the SEC because they solely match subscribers’ buy and sell orders. This exempt trading venue is called an alternative trading system (“**ATS**”), which helps provide financial markets with alternative means of liquidity.⁸⁵ While an ATS is exempt⁸⁶ from registering as an exchange, registration with FINRA as a broker-dealer is a prerequisite to operating notice registration as an ATS.⁸⁷ Accordingly, becoming an ATS is not a practical alternative for a DeFi platform.

Even if a particular digital asset is not considered a security, it will likely be deemed a commodity by the CFTC. The CFTC has enforcement power over fraud in spot markets for commodities and any DeFi provider facilitating the exchange of futures or swaps on digital assets will be engaging in activity regulated by the Commodities Exchange Act enforced by the CFTC.

Consumer protection

Consumer protection laws are yet another important regulatory consideration that DeFi providers must consider. Consumer protection compliance requirements will largely depend on the financial services activities in which DeFi providers are engaged, and the persons who have control over dApp protocols. In the U.S., consumer protection laws are broad and principles-based, and provide authorities like the Consumer Financial Protection Bureau (“**CFPB**”), the Federal Trade Commission (“**FTC**”), and state attorneys general with tremendous enforcement flexibility over unfair and deceptive acts and practices (“**UDAPs**”) that are prohibited by federal and state consumer protection statutes.

A separate patchwork of state and federal consumer protection laws governs what a DeFi platform can do with customer data, and a myriad of state non-bank lending laws and licensure requirements may apply to consumer lending on DeFi platforms. Federal laws like the Equal Credit Opportunity Act, the Fair Credit Reporting Act, and the Truth in Lending Act additionally protect financial services consumers against discriminatory, unfair, or inaccurate credit, lending, and billing practices.

Some observations

The inescapable conclusion when considering the intersection of current financial regulation in the U.S. and DeFi as it now stands is that the twain will simply never meet in their current formulations. Regulation requires a person or entity to take responsibility for a particular activity or business; DeFi fundamentally rejects the idea that anyone could or should have that level of control over a protocol. Regulators in the U.S. who are concerned about activity taking place on DeFi platforms can attempt to pursue enforcement actions against

individuals or entities either profiting from the platforms or (more likely) exhibiting control over the platforms (as discussed above). In extreme circumstances, U.S. persons may even be prohibited from interacting with certain protocols. However, once a DeFi platform is truly decentralized, and as long as the activity on the platform involves only digital assets not owned or controlled by centralized parties (such as a centralized digital asset exchange), practical enforcement options may be limited.

Rather than regulation by prohibition, which is unlikely to be particularly effective, an alternative approach would be for regulators to accept the inevitability of DeFi and seek to meet protocols “halfway.” For example, regulators could help promulgate standards that smart contracts running on a DeFi protocol should meet. This could include published code audits by identified qualified parties who meet recognized independence standards and a public repository not only of the open-source code but also easy-to-understand summaries of what the code does and any flaws or vulnerabilities that have been identified. In addition, centralized entities that are subject to regulatory oversight could provide “ratings” or other analysis of DeFi protocols that would be published and available for examination by potential users (similar to the activities currently undertaken by credit rating agencies with respect to debt securities). In addition, in order for a protocol to be available to users in the U.S., a fund could be required to be established that would be available to reimburse users under certain (limited) circumstances.

At this juncture, perhaps the most important issue facing the DeFi community is whether DeFi can scale beyond dealing in purely digital assets. While DeFi platforms could likely continue indefinitely by utilizing only digital assets (at least in certain friendly jurisdictions), for the time being, this is a fairly constrained market – total market capitalization for all cryptocurrencies remains well under \$500 billion.⁸⁸ “Real world” financial assets like residential mortgage loans, trade receivables and other similar high-quality assets are counted in the trillions of dollars and make an enticing target for DeFi protocols, creating the potential for vast scaling opportunities. At the same time, once DeFi moves from the purely digital world of fully deterministic smart contracts to assets that require real-world resources (and judicial processes) to enforce, all of the regulatory considerations discussed above move from being considered (rightly or wrongly) as “theoretical” concerns for many participants to becoming very practical issues. This is particularly true for the many regulations created after the Great Financial Crisis to address issues in the securitization and asset-backed securities markets,⁸⁹ which the use of “real world” assets in DeFi closely resembles.

What does the future hold for DeFi?

Perhaps the only thing that can be said with certainty about the DeFi space is that it is still in its very early infancy. On the positive side, the market has strongly validated many DeFi business models, driving up prices of relevant digital assets and sparking tremendous interest among venture capital firms and other investors. More and more digital assets are being locked in DeFi protocols to create yield for their owners. New and creative DeFi platforms are emerging at a rapid rate to respond to market needs. Perhaps most importantly, DeFi speaks a global language – profit, and adherents of DeFi can be found in jurisdictions around the world.

On the other hand, to date, DeFi platforms have largely ignored most of the regulatory issues discussed above. Despite its rapid growth, DeFi is still very small in size when compared to traditional finance. In order for DeFi platforms to scale as their backers and

proponents hope, there will come an inevitable clash with the policy concerns that underlie the regulatory frameworks described above, particularly if DeFi starts to incorporate “real world” assets into its fold. Answers as to how regulation and decentralization can be balanced may be found – perhaps through some of the recommendations set out above. DeFi proponents are hoping that happens before they find themselves humming along to the lyrics of the Bobby Fuller Four’s classic song, “I Fought the Law (and the Law Won).”⁹⁰

* * *

Endnotes

1. See DeFi Pulse for statistics regarding total value locked in decentralized finance protocols. <https://defipulse.com>. Total value locked (“TVL”) quoted herein is as of August 9, 2020.
2. *Id.* as of May 27, 2020.
3. See Heasman, Will, *DeFi Platforms are Handing out \$25 Million a Month*, Decrypt, July 7, 2020, available at <https://decrypt.co/34831/defi-platforms-are-handing-out-25-million-a-month>.
4. Recently, platforms like MakerDAO have experimented with using traditional “real world” assets as well, although this development is still in very nascent stages. See Orcutt, Mike, *MakerDAO Community Greenlights First ‘Real-World’ Assets for Use as Collateral*, The Block, June 8, 2020, available at <https://www.theblockcrypto.com/linked/67675/makerdao-community-vote-real-world-assets>.
5. “**Composability**” is the concept that different protocols can serve as building blocks used by developers in different combinations to serve different functions.
6. A decentralized network uses some form of distributed ledger technology (“**DLT**”) to create a ledger that is maintained simultaneously and synchronously across a dispersed group of separate computers or servers (called “**nodes**”) that all run a common (or similar) version of the related protocol software. The ledger created and maintained by this network contains a record of the transaction outcomes on the network, as determined by the protocol software. These records are duplicated across all nodes on that network (often thousands of times), producing a complete and, generally speaking, immutable record of those transaction outcomes. Unaffiliated operators of nodes in an open (non-permissioned) network may be incentivized to participate through the periodic award of digital assets native to the relevant network, whereas in a permissioned network, incentives to participate generally occur outside of the protocol software itself. Blockchain networks are one type of DLT that utilize cryptography to protect transaction information and which store transaction data sequentially in groups of transactions, called blocks, on the transaction ledger (this ordered and grouped set of transaction outcomes in what is commonly referred to as a “**blockchain**”).
7. “**Consensus mechanism**” refers to the way a group of nodes that make up a computer network can reach agreement on the state of a ledger (*i.e.*, the most current record of validated transactions) using algorithmic protocols. For example, in the Bitcoin network, nodes use the most recent validated block of the longest chain of which they are aware to commence the process of validating a new block of transactions.
8. FSB Report on Financial Stability, Regulatory, and Governance Implications of Decentralised Financial Technologies, Fin. Stability Bd. at 6–7 (June 6, 2019), <https://www.fsb.org/2019/06/decentralised-financial-technologies-report-on-financial-stability-regulatory-and-governance-implications>.
9. *Id.*

10. See <https://makerdao.com/en/>.
11. See <https://0x.org/>.
12. See <https://compound.finance/>.
13. See <https://aave.com/>.
14. See <https://balancer.finance/>.
15. See <https://dydx.exchange/>.
16. See “The Nature of the Firm,” Ronald Coase, *Economica*. Blackwell Publishing (1937).
17. See “The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations,” Ori Brafman and Rod Beckstrom, Portfolio Publishers (2006).
18. See, e.g., <https://community-development.makerdao.com/governance/governance>.
19. This includes “recursive loops” that have a particular vulnerability to exploitive attacks.
20. See Summary Overview of Stablecoins & the Law Regarding Stablecoins, Commodity Futures Trading Comm’n Tech. Advisory Comm., Subcomm. on Virtual Currencies (Oct. 3, 2019), https://www.cftc.gov/media/2731/TAC100319_Stablecoins/download.
21. A number of exciting projects involving stablecoins are being pursued by large financial institutions and others that might accelerate the adoption of digital currency. For example, JPMorgan Chase announced plans early in 2019 to issue its own fiat-backed stablecoin with a fixed redemption value: the JPM Coin. Also in 2019, six international banks signed letters of intent to issue a stablecoin on World Wire, a public blockchain payments network operated by IBM in partnership with the Stellar payments network. The new IBM stablecoin will be interoperable among subscribing banks and allow for cheap, instantaneous money transfers among institutional and potentially retail clients. Facebook’s Calibra are planning more ambitious, retail stablecoin projects intended not for interbank transfers but for widespread public use. If issued on a large scale, a retail stablecoin could be used for high-volume, small-value payments for everyday use. A retail stablecoin could not only make cross-border payments cheaper and more efficient, but also better serve unbanked persons. A stablecoin could give unbanked persons in low-income communities a means to receive, store, and exchange value without the expensive fees associated with maintaining low dollar amounts in a bank account.
22. A Vault was formerly referred to as a “Collateralized Debt Position.”
23. The stability fee is used by the Maker protocol to expand and contract the supply of Dai to maintain the pegged value of each Dai at \$1. The stability fee is akin to an interest rate with a determinable annual percentage rate (“APR”) and is a key rate in the Maker crypto-asset ecosystem. In an economically rational system, the stability fee will always exceed the interest rates payable by other DeFi lenders on Dai deposits. If not, then savvy users of DeFi protocols could obtain fee value by generating as much Dai as possible and depositing that Dai to earn interest on another platform that exceeds the associated stability fee – the cost of generating that Dai. For a more in-depth discussion of the economics, see Tetek, Josef, *Rise of the Cryptodollar Interest Rate* (February 13, 2020), <https://bankless.substack.com/p/rise-of-the-cryptodollar>.
24. See <https://community-development.makerdao.com/makerdao-mcd-faqs/faqs/vault#what-is-the-collateralization-ratio>.
25. See <https://community-development.makerdao.com/makerdao-mcd-faqs/faqs/liquidation#what-is-the-liquidation-ratio>.
26. See <https://community-development.makerdao.com/makerdao-mcd-faqs/faqs/liquidation>.
27. See <https://oasis.app/>.
28. “ERC-20” refers to a particular standard interface for digital tokens on the Ethereum blockchain that allows such tokens to be transferred between users, wallets and dApps. See <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>.

29. See 0x Whitepaper, *0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain* (Feb. 2017), https://0x.org/pdfs/0x_white_paper.pdf.
30. The regulatory implications of this are discussed below.
31. See Compound Whitepaper, *Compound: The Money Market Protocol* (Feb. 2019), <https://compound.finance/documents/Compound.Whitepaper.pdf>.
32. Compound money markets are unique to Ethereum assets like ether and ERC-20 stablecoins and ERC-20 “utility tokens.”
33. A holder of BTC would have to first obtain wrapped BTC (“**wBTC**”), an ERC-20 token minted by one of a group of merchants after the merchant has verified the BTC holder’s identity and taken custody of the BTC. wBTC is minted one-to-one for the BTC deposited with the merchant or a custodian acting on behalf of the merchant. wBTC is redeemable back to a merchant one-to-one for BTC. wBTC is a bridge to the Ethereum blockchain for BTC and allows BTC value to access various DeFi protocols built using the Ethereum network.
34. See <https://medium.com/compound-finance/compound-community-ownership-ee0ed1252cc3>.
35. See <https://medium.com/compound-finance/compound-governance-decentralized-b18659f811e0>.
36. “Gas” is the term used in the Ethereum protocol to refer to the fee to be paid to run smart contract code on the “Ethereum Virtual Machine.” Generally speaking, the more complex the operation called for by the smart contract code and the greater the demand on the Ethereum network at any given time, the higher the gas price that must be paid. Gas prices are paid with ETH.
37. See https://medium.com/@whiterabbit_hq/black-thursday-for-makerdao-8-32-million-was-liquidated-for-0-dai-36b83cac56b6. It should be noted that, if the Uniform Commercial Code were to be applied to these liquidations, a variety of safeguards would impact the manner in which a secured party is able to dispose of the relevant collateral.
38. A report from Blocknative, a digital asset analytics firm, analyzing activity in the Ethereum “mempool” found evidence of manipulation suggesting the MakerDAO Black Thursday liquidations were engineered by sophisticated actors. The mempool is a “waiting area” for transactions on the Ethereum blockchain. Some transactions are not executed and never appear on-chain, but those attempted transactions do appear in the mempool before they are evicted. Mempool data are ephemeral, but there are services, such as Blocknative, that capture and maintain this data. See <https://blog.blocknative.com/blog/mempool-forensics>.
39. See Executive Order 12614, *Presidential Task Force on Market Mechanisms*, 52 FR 43045 (November 5, 1987).
40. See *Report of the Presidential Task Force on Market Mechanisms* (January 1988) at 66.
41. The original circuit breakers were triggered by a particular drop in points on the Dow Jones Index and the SEC has modified them several times since then.
42. Absent some form of network security, blockchain networks are vulnerable to “Sybil attacks” where one actor (or group of affiliated actors) floods the network with a large number of pseudonymous identities with the intention of gaining control over the network.
43. Other alternative consensus mechanisms currently in use or under development include: Proof of Authority (“**PoA**”); Proof of Activity (“**PoAc**”); Proof of Burn (“**PoB**”); Proof of Capacity (“**PoC**”); Proof of Elapsed Time (“**PoET**”); Proof of Importance (“**PoI**”); Directed Acyclic Graphs (“**DAGs**”); Federate Byzantine Agreement (“**FBA**”); and Practical Byzantine Fault Tolerance (“**PBFT**”).

44. “**Staking**” is a form of restricted ownership whereby validators commit funds in the form of digital assets to the underlying system; validators lock their digital assets in bonded wallets, preventing them from transacting with those digital assets while they are staked. If the validator does not mint a block in accordance with the requirements of the relevant protocol, the staked digital assets will be confiscated (or “**slashed**”) by the protocol.
45. In a Sybil attack, an attacker creates a large number of accounts to trick a network into thinking that several individual accounts are participating in the network, when in fact they are all controlled by the attacker. Sybil attackers can manipulate and abuse the resources of a network. Decentralized networks are particularly prone to Sybil attacks due to their permissionless nature. *See* Zheng, S. “Mapping out Sybil Resistance Mechanisms,” *The Block*, January 15, 2019, available at <https://www.theblockcrypto.com/amp/genesis/7365/mapping-out-sybil-resistance-mechanisms>.
46. The network protocol programmatically fixes staking inflation rates. Some networks make inflation rates variable, where the inflation rate will decrease as the participation rate increases.
47. Regardless of whether a StaaS provider is simply delegated the holder’s validation rights or actually takes custody of the holder’s digital assets, the StaaS provider merely engages the holder as its customer. Either way, the holder remains the legal and beneficial owner of her staked digital assets at all times in the process.
48. A StaaS provider thus offers three core services: (i) arranging transactions using software to stake the underlying network’s native digital assets; (ii) monitoring nodes to ensure they remain online, ready to validate any given block; and (iii) continuously verifying transactions on the network to earn Rewards on its customer holder’s behalf. The StaaS provider will also often offer to its customer holders a number of different software services, including security, customer service, dashboard and interface services, system monitoring and alerts, and reward audits and distribution.
49. This chapter does not address tax issues raised by DeFi platforms, but participants in DeFi should consider the potential tax implications of their participation.
50. For example, in a widely read 2017 article, Vitalik Buterin, a co-founder of Ethereum, posited that there were three separate types of decentralization to consider, “architectural decentralization,” “political decentralization,” and “logical decentralization.” Buterin, V., *The Meaning of Decentralization*, Medium (February 6, 2017) available at <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>.
51. *S.E.C. v. W.J. Howey Co.*, 328 U.S. 293 (1946).
52. *See* FinHub, *Framework for “Investment Contract” Analysis of Digital Assets (the “Framework”)*, April 3, 2019.
53. *See, e.g., In the Matter of Zachary Coburn* (Securities Exchange Act Rel. No. 84553) (November 8, 2018) (the “**Coburn Order**”).
54. *Id.*
55. *Id.*
56. It is notable that the settlement with the SEC came after Mr. Coburn had already disposed of his interest in EtherDelta to one or more undisclosed parties and so the consent order did not directly impact the protocol. *See* <https://etherdelta.com/>. This highlights one of the most basic challenges of regulating DeFi protocols – regulators have to be able to identify someone over whom they have jurisdiction to regulate.
57. 12 C.F.R. pt. 1310 (2020). Of course, the whole basis of DeFi is that the protocols do not need to use the courts or other traditional means to enforce their outcomes – enforcement occurs deterministically – setting up an inevitable clash with the traditional legal system.

58. LabCFTC, A Primer on Smart Contracts, Commodity Futures Trading Comm'n (Nov. 27, 2018), https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718_0.pdf.
59. There are some in the DeFi community who believe that their activity is simply outside the reach of traditional regulation. We cannot take a definitive position on this, but President Trump's recent executive order relating to the popular consumer app, TikTok, which, after 45 days, prohibits "any transaction by any person, or with respect to any property, subject to the jurisdiction of the United States, with ByteDance Ltd. or its subsidiaries, in which any such company has any interest" should give proponents of this view second thoughts. See "Executive Order on Addressing the Threat Posed by TikTok," August 6, 2020, available at <https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/>.
60. 5 Del. C. § 2202.
61. 5 Del. C. § 2201(1).
62. 5 Del. C. § 2241.
63. 5 Del. C. § 2202.
64. See <https://www.dobs.pa.gov/Documents/Securities%20Resources/MTA%20Guidance%20for%20Virtual%20Currency%20Businesses.pdf> (indicating that virtual currency does not fall within the definition of "money" under the Pennsylvania Money Transmitter Act).
65. See RCW § 19.230.010(18) (specifically including virtual currency as a form of value equivalent to money covered by the money transmission definition).
66. It is worth considering what would happen if a particular DeFi loan was declared by a court to be "void" under applicable state law. On most DeFi platforms, there are no steps that could be taken to stop a specific smart contract from completing its execution once it has been launched.
67. FinCEN, Guidance on the Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, (May 9, 2019) (the "**2019 Guidance**"), <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.
68. *Id.* at 2.
69. *Id.*
70. 31 CFR § 1010.100(ff).
71. 31 CFR § 1010.100(mm).
72. 2019 Guidance at 4.
73. FinCEN specifically refers to "convertible virtual currency," which broadly encompasses any cryptocurrency or other digital asset with an equivalent value in fiat currency or that substitutes for fiat currency. FinCEN, Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies, FIN-2013-G001 at 1 (Mar. 18, 2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.
74. 2019 Guidance at 4.
75. *Id.* at 2–5.
76. *Id.* at 2.
77. *Id.*
78. Common DeFi business models that will qualify an Exchanger or Administrator as a money transmitter include a (1) digital wallet provider, (2) P2P Exchanger, (3) virtual currency kiosk operator, (4) decentralized virtual currency transmission application

provider, (5) provider of anonymizing services for virtual currencies, (6) virtual currency payment processor, and (7) an Internet casino that accepts or issues payments denominated in virtual currency. 2019 Guidance at 14–23.

79. *Id.*

80. *Id.*

81. *Id.*

82. *Howey*, 328 U.S. 293, 301 (1946).

83. *Id.*

84. *See Landreth Timber Co. v. Landreth*, 471 U.S. 681 at 686 (1985).

85. In the European Union, these trading venues are known as electronic communication networks (“ECNs”).

86. SEC Rule 3a1-1(a), 17 C.F.R. § 240.3a1-1(a) (2020).

87. SEC Regulation ATS, 17 C.F.R. § 242.300-242.303 (2020).

88. A separate concern about DeFi existing only in the world of digital assets is that DeFi platforms may be building up a high level of correlation and internal “systemic risk,” which could lead to an implosion of value if triggered by an event such as a collapse in the price of one or more key digital assets or a loss of confidence in one or more protocols due to a hack or an exploit occurring.

89. For example, the U.S. and European risk retention or “skin in the game” regulations.

90. *See* <https://www.youtube.com/watch?v=OgtQj8O92eI>.



Lewis Cohen

Tel: +1 202 754 2012 / Email: lewis.cohen@dlxlaw.com

Lewis provides in-depth legal counsel to startups, major enterprises, and governmental entities on a broad range of matters involving the use of blockchain, cryptocurrencies and other disruptive technologies. He is passionate about the ability of innovative technologies to change the way businesses and individuals work together, and is a major advocate for the potential of emerging technologies to benefit and transform industries around the globe.

Lewis brings more than 20 years of experience as a traditional capital markets and finance partner at two Global Top 50 law firms and is a frequent public speaker on the topic of blockchain and distributed ledger technology. Lewis is also recognized by *Chambers Global* as one of only three lawyers in “Band 1” for Legal: Blockchain & Cryptocurrencies – USA.



Angela Angelovska-Wilson

Tel: +1 202 365 1448 / Email: angela@dlxlaw.com

Angela is an early distributed ledger technology adopter and a leading authority in the evolving global legal and regulatory landscape surrounding distributed ledger technology and smart contracts. Prior to co-founding DLx Law, Angela served as the Chief Legal & Compliance Officer of Digital Asset and was part of the founding team. Prior to joining Digital Asset, Angela was a partner at Reed Smith where she regularly advised clients on the implementation of new technologies to finance and the complex regulatory schemes involved in the development, creation, marketing, sale and servicing of various financial services and products. Before Reed Smith, Angela spent most of her career in various roles at Latham & Watkins, where she was recognized by *The Legal 500 US* among the top finance attorneys in the U.S.



Greg Strong

Tel: +1 302 766 5535 / Email: greg.strong@dlxlaw.com

Greg advises clients on compliance with securities laws, commodities laws, and other laws and regulations that may apply to activities involving blockchain and digital assets. He has successfully represented clients before the Securities and Exchange Commission, and various other regulators. In addition, he has worked on a variety of cutting-edge transactions involving digital assets.

Prior to joining DLx Law, Greg was a Deputy Attorney General in the Delaware Department of Justice from 2003 to 2018. During that time, Greg served as the Director of Investor Protection for the State of Delaware for three years and was responsible for administering and enforcing Delaware securities laws. Greg also served as the Director of the Consumer Protection Unit for three years.

DLx Law

4913 43rd St. NW, Washington, D.C. 20016 / 114 East 25th Street, New York, NY 10010 /

1007 N. Orange Street, Wilmington, DE 19801, USA

Tel: +1 212 994 6845 / URL: www.dlxlaw.com

Legal issues surrounding the use of smart contracts

Stuart Levi, Cristina Vasile & MacKinzie Neal
Skadden, Arps, Slate, Meagher & Flom LLP

“Smart contracts” are a critical building block in the development and evolution of many types of transactions executed on distributed ledger technologies such as blockchains.¹ By automating processes and increasing outcome certainty, smart contracts can offer important benefits in a system by leveraging computer networks to process transactions. This chapter examines whether smart contracts are enforceable legal agreements under contract law in the United States, and highlights certain legal and practical considerations that will need to be addressed before smart contracts can be widely adopted in commercial contexts.

Smart contracts: An introduction

“Smart contract” is a term used to describe computer code that automatically executes all or parts of the transaction steps of an oral or written agreement between two parties. The code can either be the sole manifestation of the agreement between the parties (“code-only smart contracts”) or a complement to a traditional natural language-based contract by effectuating certain provisions of that contract (“ancillary smart contracts”). The critical difference between smart contracts and natural language contracts is how they handle performance: natural language contracts generally rely on the parties to perform the contract’s obligations, whereas smart contracts perform the parties’ obligations automatically once triggered. By eliminating the need for human intervention, smart contracts potentially reduce the execution and enforcement costs of the contract process. As a basic example, consider an agreement between an insurer and a farmer, where the insurer will pay the farmer in the event temperatures drop below a certain degree. In a natural language contract, the farmer would need to check the temperature each day, make a claim to the insurer if the temperature falls below the agreed-upon degree, and then wait for the insurer to verify the claim and pay the farmer (or dispute the claim). If a smart contract component was added, the parties could create a smart contract that automatically received a feed of the official recorded temperature (using a measure agreed by the parties) and then automatically transfer funds from the insurer’s account to the farmer’s account if the temperature drops below the agreed-upon level. Such a transfer would occur regardless of the insurer’s or farmer’s actions and without the need for either party to rely on a third-party institution or intermediary to complete the transaction.

Standards organizations and trade associations have acknowledged the impact that smart contracts could have on transactions in their areas. For example, in its latest guidance on smart derivative contracts, the International Swaps and Derivatives Association (“ISDA”) cited various ways in which smart contracts could create efficiencies in the derivatives context, particularly with respect to interest rate derivatives. However, ISDA did note that

any use of smart contracts must comply with existing legal requirements such as ISDA's documentation standard.²

The concept of smart contracts was first articulated by the computer scientist and cryptographer, Nick Szabo, and predates the development of blockchain technology.³ Since then, the ability to store immutable code and data in a transparent way on a blockchain, and the interest in disintermediating human intervention, has generated widespread interest in developing smart contracts. In the blockchain context, smart contract code is replicated across multiple nodes and executed according to the same consensus mechanism on a blockchain. Moreover, because smart contracts use the same asymmetric cryptography, in which users rely on private keys and public keys, as other blockchain-based transactions, smart contracts allow parties to authenticate each other, and provide a level of security not present in many other automated transactions.

Although smart contracts have great potential to reduce transaction costs and minimize outcome uncertainty, they currently can replace only the types of contractual provisions that can be represented in specific and objective terms, such as "if X occurs, then execute step Y." Subjective provisions, such as whether a party used commercially reasonable efforts, cannot be translated into smart contracts. In this respect, smart contracts are not particularly "smart," as they cannot parse a contract's subjective requirements or analyze a contract's provisions. It is therefore important not to confuse smart contracts with efforts being made in the areas of artificial intelligence, machine learning and quantum computing.

In addition, smart contracts will often need to rely on external (*i.e.*, "off-chain") resources before they can execute a transaction. In the crop insurance example above, the recorded temperature would be such an off-chain resource. The reliance on off-chain resources presents several problems. For example, smart contracts cannot "pull" data from off-chain resources; rather, that data must be "pushed" to the smart contract, so the parties need to agree on a single, definitive, off-chain resource willing to and capable of pushing relevant data to the smart contract. Without such clarity, there would not be a consensus between the parties as to whether the contract should trigger, and the transaction would not execute. In our example, the farmer may argue that the weather service he consulted recorded a temperature of 31 degrees, while the insurer might claim a temperature of 33 degrees.

In order to address these issues, parties to smart contracts use "oracles"—trusted third parties that retrieve mutually agreed off-chain information and then push that information to the smart contract at predetermined times. While oracles represent an elegant, and for the time being necessary, solution to smart contracts' functional need to access off-chain resources, they introduce a potential point of failure in what might otherwise be a fully automated and decentralized transaction system. An oracle might cease conducting business, experience a system failure, be hacked, or provide erroneous data. Indeed, a hacker looking to impact smart contracts would likely have an easier time exploiting the oracle's data feed than hacking the smart contract itself.

Are smart contracts legally enforceable under contract law in the United States?⁴

Although the concept of smart contracts is not new, the use of smart contracts is still in its incipient stages. As a result, there is no case law precedent that directly addresses the enforceability of smart contracts and, as discussed below, there are only a handful of state statutes purporting to address this issue directly.⁵ However, the fact that smart contracts are not drafted in natural language prose should not impact their enforceability under the principles generally applicable to contracts.

The Uniform Commercial Code and statute of frauds

As a preliminary matter, in order to be legally enforceable, smart contracts must comply with applicable state writing and signing requirements. The most relevant requirements in this respect flow from two sources: the Uniform Commercial Code (“U.C.C.”), a comprehensive set of laws governing all commercial transactions in the United States; and state laws that identify agreements that must be in writing and signed to be enforceable (referred to as the “statute of frauds”). The U.C.C. has been adopted in whole or in part by all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands; and all states except Louisiana have adopted a statute of frauds.

The “written agreement” requirement

Under the U.C.C. and statute of frauds, not every contract needs to be in writing. Under the U.C.C., the following contracts generally must be in writing: (i) a contract for the sale of goods priced at or over \$500;⁶ (ii) lease contracts relating to personal property requiring total payments of \$1,000 or more;⁷ and (iii) certain agreements that create a security interest.⁸ The specifics of what terms must be in writing vary by the subject matter. For example, a contract for the sale of goods must generally specify the goods at issue and may also include the price,⁹ while a lease must generally include the required payments, the term, and a reasonable description of the leased property.¹⁰ Similarly, each state’s statute of frauds generally requires a written agreement for: (i) agreements relating to executorship, suretyship, marriage; (ii) performance to be undertaken over one or more years after the execution of the agreement; and (iii) agreements for the sale of an interest in land.¹¹

One of the questions the U.C.C. presents is whether a smart contract, effectively a piece of computer code, can satisfy the writing requirement under the U.C.C. and statute of frauds. Historically, courts have recognized that under the U.C.C., a written agreement does not necessarily need to be natural language prose.¹² Indeed, the U.C.C. specifies that any type of “intentional reduction to tangible form” is sufficient.¹³ This is consistent with the U.C.C. policy that the “writing” requirement is meant to assure that the intention of the parties is manifest. Thus, courts have held, for example, that emails can satisfy the U.C.C. “writing” requirement.¹⁴ Courts should treat smart contracts no differently than other forms of electronic records. This is not to say that all smart contracts, by definition, will satisfy the U.C.C. requirement. Just as an email may be inconclusive as to what the parties actually intended, so too a smart contract may be too vague. That said, given the objective nature of smart contract code and the parameter certainty required to effectuate a transaction, most smart contracts for the sale of goods or for leases should satisfy the U.C.C. “writing” requirement, particularly if the parties use an ancillary smart contract where the code just executes certain terms in the natural language agreement.

A similar analysis can be applied under the statute of frauds. Under these state laws, a valid writing need not be written entirely in natural language prose nor be comprehensive.¹⁵ As with contracts interpreted under the U.C.C., courts have taken an expansive view as to what can satisfy the “writing” requirement under the statute of frauds, focusing on the intent of the parties to create a binding agreement.¹⁶ Thus, terms conveyed through email or even types of telegraphic code can form binding contracts.¹⁷

In addition, the writing under the statute of frauds generally need only contain the agreement’s “essential terms” which can vary depending on the type of transaction.¹⁸ As noted above, given the nature of smart contracts, the “essential terms” (such as price and what is being delivered) will likely be captured by the code itself. And, even if the essential terms are not capable of being expressed in “if-then” terms within the code, smart contracts can be used as ancillary tools to natural language contracts that include those terms.

The signature requirement

Both the U.C.C. and the statute of frauds require that a contract have valid signatures to be binding. This requirement can also be satisfied when using smart contracts. The U.C.C. specifies that a signature can be “any symbol executed or adopted with present intention to adopt or accept a writing.”¹⁹ Similarly, the statute of frauds generally recognizes that a signature may be any symbol made by a party with the present intent to authenticate a writing or contract.²⁰ Courts typically look to the intent of the parties and whether the signing parties proffered a signature with an intention to authenticate the writing.²¹ Since smart contract transactions on a blockchain need to be affirmatively authenticated by each party using public-private key cryptography, a digital signature on a smart contract should constitute a “symbol executed or adopted with present intention to adopt or accept a writing”²² and satisfy the flexible signature requirements of the U.C.C. and statute of frauds.

The E-SIGN Act and UETA

The Electronic Signatures in Global and National Commerce Act (“E-SIGN Act”) and state laws modeled on the Uniform Electronic Transactions Act (“UETA”) also provide important support for the concept that smart contracts should be treated as legally enforceable agreements. Under each of these acts, electronic records and electronic signatures used in interstate or foreign commerce transactions generally cannot be denied legal effect solely because they are in electronic form.²³ Although the E-SIGN Act is a federal law, and generally preempts state laws, individual states may “modify, limit, or supersede”²⁴ the E-SIGN Act if they adopt UETA or satisfactory “alternative procedures or requirements.”²⁵ UETA has been adopted by 47 states, the District of Columbia, Puerto Rico and the Virgin Islands.

The key question is whether the blockchains on which smart contracts are stored are “electronic records” and therefore enjoy protection under these acts, and whether the digital signatures used with smart contracts can be deemed protectable “electronic signatures.”

Both the E-SIGN Act and UETA define electronic records broadly to include any “record created, generated, sent, communicated, received, or stored by electronic means.”²⁶ An explanatory comment to UETA indicates that this includes any “[i]nformation processing systems, computer equipment and programs . . . and similar technologies” and any “information stored on a computer hard drive.”²⁷ There should be little dispute that a blockchain satisfies this broad definition since, at a minimum, it stores records by electronic means. Moreover, at least one court has suggested that a database is an electronic record under UETA,²⁸ providing important guidance given that a blockchain is an encrypted and distributed database.

The E-SIGN Act and UETA also define electronic signatures broadly. Under both acts, an “electronic signature” includes any “electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.”²⁹ Moreover, UETA expressly states that this definition encompasses a “digital signature using public key encryption technology.”³⁰ As with the statute of frauds and the U.C.C., a digital signature based on asymmetric cryptography that is used to sign a smart contract should meet the E-SIGN Act and UETA definition of a legally valid electronic signature.

The E-SIGN Act and UETA also include an additional concept that supports the enforceability of smart contracts. Under these acts, an agreement cannot be denied legal effect because the parties used an “electronic agent” which each act defines to include a “computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.”³¹ Smart contracts that run self-executing code previously agreed to by the

contracting parties would seem to fit squarely within this definition. The comments to UETA also contemplate the possibility that electronic agents could conduct transactions with other electronic agents or autonomously, which could occur as smart contracts and artificial intelligence continue to develop.³²

In order to rely on the foregoing protections of UETA, the parties must first agree in a non-electronic writing that they will conduct all or part of a transaction electronically. Thus, one party could not implement a smart contract without the express written consent of the other party. Similarly, if a written record needs to be made available to a consumer, the E-SIGN Act requires affirmative consumer consent before an electronic record can be used, which consent can be withdrawn at any time.³³ The right for consumers to withdraw their consent at any time under the E-SIGN Act may create operational complications given the self-executing nature of most smart contracts.

As noted above, only 47 states have adopted UETA. Illinois (through the state's Electronic Commerce Security Act),³⁴ New York (through the state's Electronic Signatures and Records Act),³⁵ and Washington (through a state statute that recognizes the E-SIGN Act as applying to state and local transactions)³⁶ have each adopted their own unique e-signature statutes *in lieu* of a statute modeled on UETA. While these three states adopt broad definitions of electronic records and electronic signatures, none offer the added protection of electronic agents set forth in the 47 states that have adopted UETA.

Specific state laws applicable to smart contracts

Although, as discussed above, there are strong arguments that existing state laws already provide a sound basis for the enforceability of smart contracts, to date, six states have amended their laws specifically to allow for the enforceability of blockchain-based contracts, and many other states have enacted laws that recognize blockchain technology and blockchain-based legal instruments.³⁷ With respect to laws that allow for the enforceability of blockchain-based contracts, many believe that these states have enacted such laws in order to appear “blockchain friendly” to attract blockchain-based companies. However, in their attempts to provide greater clarity on this issue and incentivize blockchain-based development, these states may have created more uncertainty, in part because of how these laws will be interpreted and in part because of the implicit suggestion that existing laws did not cover smart contract transactions. Moreover, as an increasing number of states adopt different definitions for the same terms, the potential for disputes between parties relying on smart contracts increases and the determination of which state's law governs becomes more important.

Arizona

In March 2017, Arizona became the first state to amend its version of UETA, the Arizona Electronic Transactions Act (“AETA”), to address blockchain technology. AETA as amended provides that a “signature that is secured through blockchain technology is . . . an electronic signature,” and a “record or contract that is secured through blockchain technology is . . . an electronic record.”³⁸ AETA further states that “[s]mart contracts may exist in commerce” and that contracts “may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term.”³⁹ “Blockchain technology” is defined to mean “distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth.”⁴⁰ “Smart contract” is defined as “an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct

transfer of assets on that ledger.”⁴¹ Although these definitions are broad, they employ multiple ambiguous terms whose exact meaning litigants and courts may debate.

Arkansas

In July 2019, Arkansas amended its version of UETA to include definitions for “blockchain distributed ledger technology,” “blockchain technology” and “smart contracts.” Under the amendment, “blockchain distributed ledger technology” means “technology that uses a distributed, decentralized, shared and replicated ledger that is either public or private, permissioned or permissionless and that contains data that is securely protected with cryptography, immutable, auditable and provides an uncensored truth.”⁴² “Blockchain technology” means “a shared, immutable ledger that facilitates the process of recording one (1) or more transactions and tracking one (1) or more tangible or intangible assets in a business network,”⁴³ and “smart contract” means “(A) [a] [b]usiness logic that runs on a blockchain; or (B) [a] software program that stores rules on a shared and replicated ledger and uses the stored rules for: (i) [n]egotiating the terms of a contract, (ii) [a]utomatically verifying the contract and (iii) [e]xecuting the terms of a contract.”⁴⁴ A signature that is secured through blockchain technology is considered to be an electronic record and any smart contract is considered to be a commercial contract.⁴⁵ Similar to the Arizona legislation, the definitions are broad, yet significantly vague. In addition, the definitions of blockchain technology and smart contract noticeably differ from the other states. It is not clear, for example, what the statute means when it describes smart rules for *negotiating* the terms of a contract (emphasis added).

Illinois

In January 2020, Illinois passed the Blockchain Technology Act (“BTA”), a law directly targeted at blockchain technology and smart contract enforceability. Under BTA, “a smart contract, record or signature may not be denied legal effect or enforceability solely because a blockchain was used to create, store, or verify [it].”⁴⁶ Further, if a law requires a record to be in writing, “submission of a blockchain which electronically contains the record” satisfies such law and, if a law requires a signature, “submission of a blockchain which electronically contains the signature or verifies the intent of a person to provide the signature satisfies such law.”⁴⁷ “Blockchain” is defined to mean “an electronic record created by the use of a decentralized method by multiple parties to verify and store a digital record of transactions . . . secured by the use of a cryptographic hash of previous transaction information.” BTA also defines “cryptographic hash” to mean “a mathematical algorithm which performs a one-way conversion of input data into output data of a specified size to verify the integrity of the data.”⁴⁸ Under BTA, a “smart contract” is defined as “a contract stored as an electronic record which is verified by the use of a blockchain.”⁴⁹

BTA also sets forth clear limitations on the use of blockchain technology. For example, in the presence of a law that requires a certain contract or record be in writing, the legal enforceability of such record or contract may be denied if the smart contract is “not in a form that is capable of being retained and accurately produced for later reference” by the relevant parties.⁵⁰ BTA also states that blockchain technology cannot satisfy legal requirements for posting, displaying or communicating records, nor can it satisfy legal requirements that a document be in writing if it relates to the transportation or handling of hazardous materials, pesticides or other toxic or dangerous materials.⁵¹ Finally, BTA sets limits on notice requirements in smart contracts that relate to termination of service by a public utility; defaults, foreclosures, evictions, and other real property rights; cancellation of a policy related to health insurance; or the recall or material failure of a product that risks

endangering the health or safety of a person.⁵² While BTA does provide clarity with respect to the enforceability of smart contracts and their limitations, its definition of smart contract is vague, and leaves ambiguous how litigators and courts will interpret its meaning.

Nevada

In June 2017, Nevada amended its version of UETA, the Nevada Electronic Transactions Act (“NETA”) to state that an “electronic record” includes, without limitation, a blockchain.⁵³ The statute defines “blockchain” to mean “an electronic record of transactions or other data which is: (a) [u]niformly ordered; (b) processed using a decentralized method by which one or more computers or machines verify the recorded transactions or other data; (c) [r]edundantly maintained by one or more computers or machines to guarantee the consistency or nonrepudiation of the recorded transactions or other data; and (d) [v]alidated by the use of cryptography.”⁵⁴ In a later amendment in October 2019, NETA clarified that the definition of blockchain includes, without limitation, a public blockchain.⁵⁵ Smart contracts are not directly addressed in the statute, and note that the definition of blockchain is fairly different than that adopted by other states.⁵⁶

North Dakota

In August 2019, North Dakota amended its version of UETA, the North Dakota Uniform Electronic Transactions Act (“NDUETA”) such that “[a] signature secured through blockchain technology is considered to be in an electronic form and to be an electronic signature”⁵⁷ and that “[a] record or contract secured through blockchain technology is considered to be in an electronic form and to be an electronic record” and, further, that “[s]mart contracts may exist in commerce . . . [and] a smart contract relating to a transaction may not be denied legal effect, validity, or enforceability solely because the contract contains a smart contract term.”⁵⁸ NDUETA also amends the definitions to mirror Arizona’s definition of “blockchain technology,” defining it as a “distributed ledger technology that uses a distributed, decentralized, shared, and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless and which is protected with cryptography, is immutable, and auditable and provides an uncensored truth.”⁵⁹ Under the law, “smart contract” means “an event-driven program, with state, that runs on a distributed, decentralized, shared, and replicated ledger and which can take custody over and instruct transfer of assets on that ledger.”⁶⁰

Tennessee

In March 2018, Tennessee amended its UETA to clarify that “[a] record or contract that is secured through distributed ledger technology is considered to be in an electronic form and to be an electronic record.”⁶¹ It further provides: “[a] cryptographic signature that is generated and stored through distributed ledger technology is considered to be . . . an electronic signature.”⁶² Tennessee adopted some of the blockchain technology definition used by Arizona and North Dakota, but categorized it as “distributed ledger technology” and made some important modifications. Specifically, distributed ledger technology is defined as “any distributed ledger protocol and supporting infrastructure, including blockchain, that uses a distributed, decentralized, shared, and replicated ledger, whether it be public or private, permissioned or permissionless, and which may include the use of electronic currencies or electronic tokens as a medium of electronic exchange.”⁶³ Similarly, the state’s definition of “smart contracts” mirrors that of Arizona but adds some additional language. A “smart contract” is defined to mean “an event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that: (A) [t]ake custody over and

instruct transfer of assets on that ledger; (B) [c]reate and distribute electronic assets; (C) [s]ynchronize information; or (D) [m]anage identity and user access to software applications.”⁶⁴

Other legal considerations

In addition to the foregoing statutes generally governing the enforceability of contracts, smart contracts may be subject to a variety of legal frameworks depending on their terms and consideration. This may include: state and federal commodities and securities laws and regulations; anti-money laundering laws and regulations; and state money transmission laws. Developers of, and parties to, smart contracts must discern which regulations apply and what such compliance entails, including registration and documentation requirements.

Challenges with the widespread adoption of smart contracts

Given the existing legal frameworks for recognizing electronic contracts, it is quite likely that a court today would recognize the validity of code that executes provisions of a smart contract—what we have classified as ancillary smart contracts. There is also precedent to suggest that a code-only smart contract might enjoy similar legal protection. The challenge to widespread smart contract adoption may therefore have less to do with the limits of the law than with potential clashes between how smart contract code operates and how parties transact business. We set forth below certain of these challenges:

How can non-technical parties negotiate, draft and adjudicate smart contracts?

A key challenge in the widespread adoption of smart contracts is that parties will need to rely on a trusted, technical expert to either capture the parties’ agreement in code or confirm that code written by a third party is accurate. While some analogize this to hiring a lawyer to explain “the legalese” of a traditional text-based contract, the analogy is misplaced. Non-lawyers typically can understand simple short-form agreements as well as many provisions of longer agreements, especially those setting forth business terms. But a non-programmer would be at a total loss to understand even the most basic smart contract and is therefore significantly more beholden to an expert to explain what the contract “says.” Although projects are currently underway to make smart contract code more accessible, at present, non-programmer parties remain at a critical disadvantage with respect to understanding the code that governs their own agreements.

To some extent, the inability of contracting parties to understand the smart contract code will not be a hindrance to entering into ancillary smart contracts. This is because for many basic functions, text templates can be created and used to indicate what parameters need to be entered and how those parameters will be executed. For example, assume a simple smart contract function that extracts a late fee from a counterparty’s wallet if a defined payment is not received by a specified date. The text template could prompt the parties to enter the amount of the expected payment, the due date and the amount of the late fee. However, a party may want to confirm that the underlying code actually will perform the functions specified in the text, and that there are no additional conditions or parameters—especially where the template disclaims any liability arising from the accuracy of the underlying code. This review will require a trusted third party with programming expertise.

In cases where such templates do not exist, and new code must be developed, the parties will need to communicate the intent of their agreement to a programmer. Simply handing that programmer a copy of the legal agreement would be inefficient, as it would require the programmer to try to decipher a legal document. As a possible solution, parties relying on ancillary smart contracts may need to draft a separate “term sheet” of functionality that the smart contract should perform and that can be provided to the programmer.

The parties also may want written representations from the programmer that the code performs as contemplated. The net result is that for customized arrangements that do not rely on an existing template, the parties may need to enter into a written agreement with the smart contract programmer, not unlike the contract that parties may enter into with a provider of services for Electronic Data Interchange transactions today.

Insurance companies could also create policies to protect contracting parties from the risk that smart contract code does not perform the functions specified in the text of an agreement. Although the parties would also want to review (or have a third party review) the code, insurance can provide additional protection in the event the parties miss errors when reviewing the code. The parties would also take some additional comfort from the fact that the insurance company likely conducted its own code audit before agreeing to insure the code.

Code-only smart contracts used for business-to-consumer transactions could pose an additional set of issues that will need to be addressed. Courts are wary of enforcing agreements where the consumer did not receive adequate notice of the terms of the agreement,⁶⁵ and may be hesitant to enforce a smart contract where the consumer was not also provided with an underlying text agreement that included the complete terms or where the business did not build in consumer protection measures, such as ensuring proper dispute resolution mechanisms are in place.⁶⁶

Finally, as the validity or performance of smart contracts increasingly become adjudicated, courts may need a system of court-appointed experts to help them decipher the meaning and intent of the code. Today, parties routinely use their own experts when technical issues are at the center of a dispute. While both federal courts and many state courts have the authority to appoint their own experts, they rarely exercise that authority.⁶⁷ That approach may need to change if the number of standard contract disputes that center on interpreting smart contract code increases.

Liability of the smart contract developer

As noted above, in many cases, the parties to a smart contract will not have the technical capability to create a smart contract, and may therefore hire a third party to create the smart contract, or may rely on a smart contract “template” offered by a third party. In such cases, there is the possibility of programmer error or that the parties did not accurately convey what they intended to the developer. Parties will need to consider the ramifications of these situations and the appropriate allocation of risk and liability.

Developers of smart contracts may also need to be wary of their own liability in cases where smart contract code they developed is used for unlawful purposes. In October 2018, Brian Quintenz, Commissioner of the Commodity Futures Trading Commission (“CFTC”), suggested that smart contract code developers could be held accountable for aiding and abetting CFTC violations where they “could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations.”⁶⁸ In November 2018, the Securities and Exchange Commission (“SEC”) settled charges of operating an unregistered securities exchange against Zachary Coburn, the founder and developer of EtherDelta, a decentralized digital asset exchange. Although the SEC’s order appears to be based, in part, on Coburn’s control over EtherDelta’s operations and his role as founder, the order also lists the fact that Coburn “wrote and deployed the EtherDelta smart contract to the Ethereum Blockchain” as a factor in finding that Coburn caused EtherDelta to violate the Securities Exchange Act of 1934.⁶⁹

While some cases of developer liability will be clear, such as where a developer was actively part of an illegal scheme, it is likely that given the open-source nature of many blockchain projects, developers may have less insight into how their smart contract code is being used, or by whom. The CFTC has not released further guidance on how smart contracts will implicate its jurisdiction and enforcement authority.

Outside the CFTC context, jurisprudence on contributory liability in the context of peer-to-peer technologies may provide useful precedent in balancing the need to protect developers with the need to provide redress to parties that are harmed by smart contracts put to unlawful use. For example, under *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*,⁷⁰ peer-to-peer file-sharing sites are not liable for users' infringing uses if: (1) they are not distributing their product with the "object of promoting its use to infringe;" (2) they either (a) do not have actual knowledge of specific infringements, or (b) if they do have knowledge, they are not in a position to block the infringing conduct and have failed to do so; and (3) the product is capable of substantial non-infringing use.

While *Grokster* dealt with contributory infringement under copyright law, courts may apply its core principles in the context of developer liability for blockchain-based smart contracts. In order to minimize potential liability, smart contract developers should not only avoid developing smart contracts with the object of enabling illegal use, but should also use reasonable efforts to block unexpected unlawful use.

What is the "final" agreement between the parties?

When analyzing traditional text-based contracts, courts will examine the final, written document to which the parties have agreed in order to determine whether the parties are in compliance or breach. Courts have long emphasized that it is this final agreement that represents the mutual intent of the parties—the "meeting of the minds."

In the case of code-only smart contracts, the code that is executed—and the outcome it produces—represents the only objective evidence of the terms agreed to by the parties. In these cases, email exchanges between the parties as to what functions the smart contract "should" execute, or oral discussions to that effect, likely would yield to the definitive code lines as the determinative manifestation of the parties' intent.

With respect to ancillary smart contracts, a court likely would look at the text and code as a unified single agreement. The issue becomes complicated when the traditional text agreement and the code do not align. In the crop insurance example described above, assume the text of an agreement specifies that an insurance payout will be made if the temperature falls below 32 degrees, while the smart contract code triggers the payment if the temperature is equal to or below 32 degrees. Assuming that the text agreement does not state whether the text or code controls in the event of an inconsistency, courts will need to determine—perhaps on a case-by-case basis—whether the code should be treated as a mutually agreed amendment to the written agreement or whether the text of the agreement should prevail. In some respects, the analysis should be no different than a case where the provisions of a main agreement differ from what is reflected in an attached schedule or exhibit. The fact that here the conflict would be between text and computer code and not two text documents should not be determinative, but courts may take a different view.

One solution will be for parties to use a text-based contract where the parameters that trigger the smart contract execution are not only visible in the text but actually populate the smart contract. In our example, "less than 32 degrees" would not only be seen in the text, but also would create the parameter in the smart contract itself, thereby minimizing the chances of any inconsistency.

The automated nature of smart contracts

One of the key attributes of smart contracts is their ability to automatically and relentlessly execute transactions without the need for human intervention. However, this automation, and the fact that smart contracts cannot easily be amended or terminated unless the parties incorporate such capabilities during the creation of the smart contract, present some of the greatest challenges facing widespread adoption of smart contracts.

For example, with traditional text contracts, a party can easily excuse a breach simply by not enforcing the available penalties. If a valued customer is late with its payment one month, the vendor can make a real-time decision that preserving the long-term commercial relationship is more important than any available termination right or late fee. However, if this relationship had been reduced to a smart contract, the option not to enforce the agreement on an *ad hoc* basis likely would not exist. A late payment will result in the automatic extraction of a late fee from the customer's account or the suspension of a customer's access to a software program or an internet-connected device if that is what the smart contract was programmed to do. The automated execution provided by smart contracts might therefore not align with the manner in which many businesses operate in the real world.

Similarly, in a text-based contractual relationship, a party may be willing to accept, on an *ad hoc* basis, partial performance to be deemed full performance. This might be because of an interest in preserving a long-term relationship, because a party determines that partial performance is preferable to no performance at all or because of an unforeseeable external event, such as COVID-19, where a party may wish to excuse performance for a certain period of time. Here, again, the objectivity required for smart contract code might not reflect the realities of how contracting parties interact.

Amending and terminating smart contracts

At present, there is no simple path to amend a smart contract, creating certain challenges for contracting parties. For example, in a traditional text-based contract, if the parties have mutually agreed to change the parameters of their business deal, or if there is a change in law, the parties quickly can draft an amendment to address that change, or simply alter their course of conduct. Smart contracts currently do not offer such flexibility. Indeed, given that blockchains are immutable, modifying a smart contract is far more complicated than modifying standard software code that does not reside on a blockchain. The result is that amending a smart contract may yield higher transaction costs than amending a text-based contract, and increases the margin of error that the parties will not accurately reflect the modifications they want to make.

Similar challenges exist with respect to terminating a smart contract. Assume a party discovers an error in an agreement that gives the counterparty more rights than intended, or concludes that fulfilling its stated obligations will be far more costly than it had expected. In a text-based contract, a party can engage in, or threaten, so-called "efficient breach," *i.e.*, knowingly breaching a contract and paying the resulting damages if it determines that the cost to perform is greater than the damages it would owe. Moreover, by ceasing performance, or threatening to take that step, a party may bring the counterparty back to the table to negotiate an amicable resolution. Smart contracts do not yet offer analogous self-help remedies.

Projects are currently underway to create smart contracts that are terminable at any time and more easily amended. While in some ways this is antithetical to the immutable and automated nature of smart contracts, it reflects the fact that smart contracts only will gain commercial acceptance if they reflect the business reality of how contracting parties act.

Objectivity and the limits of incorporating desired ambiguity into smart contracts

The objectivity and automation required of smart contracts can run contrary to how business parties actually negotiate agreements. During the course of negotiations, parties implicitly engage in a cost-benefit analysis, knowing that at some point there are diminishing returns in trying to think of, and address, every conceivable eventuality. These parties no longer may want to expend management time or legal fees on the negotiations, or may conclude that commencing revenue-generating activity under an executed contract outweighs addressing unresolved issues. Instead, they may determine that if an unanticipated event actually occurs, they will figure out a resolution at that time. Similarly, parties may purposefully opt to leave a provision somewhat ambiguous in an agreement in order to give themselves the flexibility to argue that the provision should be interpreted in their favor. This approach to contracting is rendered more difficult with smart contracts where computer code demands an exactitude not found in the negotiation of text-based contracts. A smart contract cannot include ambiguous terms nor can certain potential scenarios be left unaddressed. As a result, parties to smart contracts may find that the transaction costs of negotiating complex smart contracts exceed that of traditional text-based contracts.

It will take some time for those adopting smart contracts in a particular industry to determine which provisions are sufficiently objective to lend themselves to smart contract execution. As noted, to date, most smart contracts perform relatively simple tasks where the parameters of the “if/then” statements are clear. As smart contracts increase in complexity, parties may disagree on whether a particular contractual provision can be captured through the objectivity that a smart contract demands.

Do smart contracts really guarantee payment?

One benefit often touted of smart contracts is that they can automate payment without the need for dunning notices or other collection expenses and without the need to go to court to obtain a judgment mandating payment. While this is indeed true for simpler use cases, it may be less accurate in complex commercial relationships. The reality is that parties are constantly moving funds throughout their organization and do not “park” total amounts that are due on a long-term contract in anticipation of future payment requirements. Similarly, a person obtaining a loan is unlikely to keep the full loan amount in a specified wallet linked to the smart contract. Rather, the borrower will put those funds to use, funding the necessary repayments on an *ad hoc* basis.

If the party owing amounts under the smart contract fails to fund the wallet on a timely basis, a smart contract looking to transfer money from that wallet upon a trigger event may find that the requisite funds are not available. Implementing another layer into the process, such as having the smart contract seek to pull funds from other wallets or having that wallet “fund itself” from other sources, would not solve the problem if those wallets or sources of funds also lack the requisite payment amounts. The parties might seek to address this issue through a text-based requirement that a wallet linked to the smart contract always has a minimum amount, but that solution simply would give the party a stronger legal argument if the dispute was adjudicated. It would not render the payment operation of the smart contract wholly automatic. Thus, although smart contracts will render payments far more efficient, they may not eliminate the need to adjudicate payment disputes.

Risk allocation for attacks and failures

Smart contracts introduce an additional risk that does not exist in most text-based contractual relationships—the possibility that the contract will be hacked or that the code or protocol simply contains an unintended programming error. Given the relative security

of blockchains, these concepts are closely aligned; namely, most “hacks” associated with blockchain technology are really exploitations of an unintended coding error. As with many bugs in computer code, these errors are not glaring, but rather become obvious only once they have been exploited. For example, in July 2017, an attacker was able to drain several multi-signature wallets offered by Parity of \$31 million in ether.⁷¹ In November of that same year, a second undetected security vulnerability activated a freeze of more than \$160 million in ether held in multi-signature wallets also offered by Parity.⁷² Multi-signature wallets add a layer of security because they require more than one private key to access the wallet. However, in the July 2017 Parity attack, the attacker was able to exploit a flaw in the Parity code by reinitializing the smart contract and making himself or herself the sole owner of the multi-signature wallets. Similarly, in the November 2017 incident, it was the same flaw that initiated a freeze of the wallets. These incidents demonstrate that parties to a smart contract will need to consider how risk and liability for unintended coding errors and resulting exploitations are allocated between the parties, and possibly with any third-party developers or insurers of the smart contract.

Governing law and venue

One of the key promises of blockchain technology, and by extension smart contracts, is the development of robust, decentralized and global platforms. However, global adoption means that parties may be using a smart contract across far more jurisdictions than might exist in the case of text-based contracts. The party offering terms under a smart contract would therefore be best served by specifying the governing law and venue for that smart contract. A governing law provision specifies what substantive law will apply to the interpretation of the smart contract, whereas a venue clause specifies which jurisdiction’s courts will adjudicate the dispute. In cases where governing law or venue is not specified, a plaintiff may be relatively unconstrained in choosing where to file a claim or in arguing which substantive law should apply given the wide range of jurisdictions in which a smart contract might be used (for example, courts may look not only where the parties are domiciled, but also to the parties’ IP addresses or where the smart contract was coded). Given that many early disputes concerning smart contracts will be ones of first impression, contracting parties will want some certainty surrounding where such disputes will be adjudicated.

Conclusion

Although smart contracts have been adopted and used, they are in their nascent stages, and therefore so is the law surrounding their enforceability and use. While there are strong arguments that properly constructed smart contracts are enforceable under existing statutes governing electronic contracts, certain issues must be resolved before they can enjoy widespread adoption in complex commercial transactions. While smart contracts have potential to change the way markets operate, their impact will invariably be shaped by how such applications fit within the contours of the law.

* * *

Endnotes

1. Blockchains are one type of “distributed ledger technology” in which data is organized in blocks and new data can only be appended to the chain. For purposes of this chapter, we refer to blockchains, but most of the legal issues presented here apply to other forms of distributed ledger technology as well.

2. See Int'l Swaps & Derivatives Ass'n, *ISDA Legal Guidelines For Smart Derivatives Contracts: Interest Rate Derivatives* (2020), <https://www.isda.org/a/I7XTE/ISDA-Legal-Guidelines-for-Smart-Derivatives-Contracts-IRDs.pdf>.
3. Compare Nick Szabo, *Smart Contracts: Building Blocks for Digital Market* (1996), with Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).
4. There is no federal contract law in the United States; rather, the enforceability and interpretation of contracts is determined at the state level. Thus, while certain core principles apply consistently across state lines, and there has been a drive to harmonize state laws by the Uniform Law Commission, any conclusions regarding the enforceability of smart contracts must be tempered by the reality that states may adopt different views.
5. For a comprehensive overview of the enforceability of smart contracts, see Cardozo Blockchain Project, "*Smart Contracts*" & *Legal Enforceability* (2018), https://cardozo.yu.edu/sites/default/files/2020-01/smart_contracts_report_2_0.pdf; see also Uniform L. Com'n, *Guidance Note Regarding the Relation Between the Uniform Electronic Transactions Act and Federal ESIGN Act, Blockchain Technology and "Smart Contracts"* (2019) (opining that state UETA provisions do not require amendment to enable use of blockchain technology and smart contracts in electronic transactions).
6. U.C.C. § 2-201.
7. *Id.* § 2A-201(1)(a).
8. *Id.* § 9-203(b)(3)(A).
9. *Id.* § 2-201.
10. *Id.* § 2A-201.
11. See, e.g., Restatement (Second) of Contracts § 110 (Am. Law Inst. 1981). Contracts that fail to comply with the statute of frauds remain enforceable in some cases, such as cases wherein promissory estoppel applies. See Restatement (Second) of Contracts § 90 (Am. Law Inst. 1981).
12. See, e.g., *Apex Oil Co. v. Vanguard Oil & Serv. Co.*, 760 F.2d 417, 420, 423 (2d Cir. 1985).
13. U.C.C. § 1-201(43).
14. See, e.g., *Bazak Int'l Corp. v. Tarrant Apparel Grp.*, 378 F. Supp. 2d 377, 383 (S.D.N.Y. 2005) ("Although e-mails are intangible messages during their transmission, this fact alone does not prove fatal to their qualifying as writings under the UCC. . . . [F]orms of communication regularly recognized by the courts as fulfilling the UCC 'writing' requirement, such as fax, telex and telegraph, are all intangible forms of communication during portions of their transmission. Just as messages sent using these accepted methods can be rendered tangible, thereby falling within the UCC definition, so too can e-mails.>").
15. See, e.g., *Bibb v. Allen*, 149 U.S. 481, 496 (1893) (holding that a contract written in telegraphic cipher code was binding); *Cloud Corp. v. Hasbro, Inc.*, 314 F.3d 289, 295–96 (7th Cir. 2002).
16. See, e.g., *Leeds v. First Allied Conn. Corp.*, 521 A.2d 1095, 1097 (Del. Ch. 1986) (explaining an agreement is binding when "a reasonable negotiator . . . would have concluded, in that setting, that the agreement reached constituted agreement on all of the terms that the parties themselves regarded as essential").
17. See, e.g., *Bibb*, 149 U.S. at 496; *Naldi v. Grunberg*, 80 A.D.3d 1, 10 (N.Y. App. Div. 2010).
18. See, e.g., *Ross v. Ross*, 172 A.3d 1069, 1075 (N.H. 2017); *Simmonds v. Marshall*, 292 A.D.2d 592, 592 (N.Y. App. Div. 2002); *Leeds*, 521 A.2d at 1097.
19. U.C.C. § 1-201(37).
20. Restatement (Second) of Contracts § 134 (Am Law Inst. 1981); U.C.C. § 1-201(37).
21. See, e.g., *SD Prot., Inc. v. Del Rio*, 498 F. Supp. 2d 576, 584 (E.D.N.Y. 2007); U.C.C. § 1-201 cmt. at 37.

22. See U.C.C. § 1-201(37); *see also* Restatement (Second) Contracts § 134.
23. 15 U.S.C. § 7001(a)(1); UETA § 7(a), (c)-(d) (1999). There are certain exceptions to these acts (such as wills) that will not impact the majority of smart contract usage.
24. 15 U.S.C. § 7002(a).
25. 15 U.S.C. § 7002(a)(2)(A).
26. UETA § 2(7); *see also* 15 U.S.C. § 7006(4).
27. UETA § 2 cmt. at 8.
28. See *Godfrey v. Fred Meyer Stores*, 124 P.3d 621, 631 (Or. Ct. App. 2005) (Armstrong, J., concurring).
29. UETA § 2(8); *see also* 15 U.S.C. § 7006(5).
30. UETA § 2 cmt. at 10.
31. *Id.* § 2(6); *see also* 15 U.S.C. § 7006(3).
32. UETA § 2 cmt. at 8.
33. 15 U.S.C. § 7001(c)(1).
34. 5 Ill. Comp. Stat. 175/5-110.
35. N.Y. State Tech. Law § 304.
36. Wash. Rev. Code § 19-360.010–360.040 (repealed by 2019 Wash. Sess. Laws 710, ch. 132).
37. Note that other states, including California, Colorado, Connecticut, Delaware, Ohio, Vermont, and Wyoming, have enacted blockchain-related laws, though these laws do not specifically address the issue of blockchain-based contracts. In addition, other states, such as Florida, Kentucky, and Virginia, have launched working groups dedicated to evaluating the impact of blockchain and how it can be leveraged in that state.
38. Ariz. Rev. Stat. Ann. § 44-7061.
39. *Id.* § 44-7061(C).
40. *Id.* § 44-7061(E)(1).
41. *Id.* § 44-7061(E)(2).
42. Ark. Code Ann. § 25-32-122(a)(1) (section numbering omitted).
43. *Id.* § 25-32-122(a)(2).
44. *Id.* § 25-32-122(a)(3).
45. *Id.* § 25-32-122(b).
46. 205 Ill. Comp. Stat. 730/10(a).
47. *Id.* at 730/10(c)-(d).
48. *Id.* at 730/5.
49. *Id.*
50. *Id.* at 730/15(a).
51. *Id.* at 730/15(e).
52. *Id.* at 730/15(d)(1)-(4).
53. Nev. Rev. Stat. Ann. § 719.090.
54. *Id.* at § 719.045(1).
55. S. 162, 80th Leg. (Nev. 2019).
56. *See also* S. 163, 80th Leg. (Nev. 2019).
57. N.D. Cent. Code Ann. § 9-16-19(1).
58. *Id.* § 9-16-19(2)-(3).
59. *Id.* § 9-16-19(5)(a).
60. *Id.* § 9-16-19(5)(b).
61. Tenn. Code Ann. § 47-10-202(b).
62. *Id.* § 47-10-202(a).

63. *Id.* § 47-10-201(1).
64. *Id.* § 47-10-201(2).
65. *See, e.g., Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 237–38 (2d Cir. 2016) (reversing the district court’s dismissal for failure to state a claim and holding that reasonable minds could disagree as to whether Amazon provided the consumer with reasonable notice of the mandatory arbitration provision at issue).
66. *See World Bank Grp., Fintech Note No. 6, Smart Contract Technology and Financial Inclusion* 17–18 (2020), <https://openknowledge.worldbank.org/bitstream/handle/10986/33723/Smart-Contract-Technology-and-Financial-Inclusion.pdf?sequence=1&isAllowed=y>.
67. *See Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure*, § 6304 (3d ed. Supp. 2011) (“In fact, the exercise of Rule 706 powers is rare under virtually any circumstances. This is, at least in part, owing to the fact that appointing an expert witness increases the burdens of the judge, increases the costs to the parties, and interferes with the adversarial control over the presentation of evidence.”); *see also Stephanie Domitrovich et al., State Trial Judge Use of Court Appointed Experts: Survey Results and Comparisons*, 50 *Jurimetrics* 371, 373–74 (2010).
68. Brian Quintenz, Comm’r, U.S. Commodity Futures Trading Comm’n, Remarks at the 38th Annual GITEX Technology Week Conference (Oct. 16, 2018), <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>.
69. *Zachary Coburn*, Exchange Act Release No. 84,553, Admin. Proc. File No. 3-18888, at 9 (Nov. 8, 2018), <https://www.sec.gov/litigation/admin/2018/34-84553.pdf>.
70. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 918–19, 936–37 (2005) (holding that one who “distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.”).
71. *See Haseeb Qureshi, A Hacker Stole \$31M of Ether – How it Happened, and What It Means for Ethereum*, freeCodeCamp (July 20, 2017), <https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce>.
72. *See Stan Higgins, Parity Floats Fix for \$160 Million Ether Fund Freeze*, CoinDesk (Nov. 13, 2017), <https://www.coindesk.com/parity-floats-fix-160-million-ether-fund-freeze>.

* * *

Acknowledgment

The authors acknowledge the tremendous assistance of Alex Lipton who was instrumental in drafting the first edition of this chapter, and is currently corporate counsel at Unite Us in New York.

**Stuart Levi****Tel: +1 212 735 2750 / Email: stuart.levi@skadden.com**

Stuart D. Levi is co-head of Skadden's Intellectual Property and Technology Group, and he coordinates the firm's blockchain, outsourcing and privacy practices. Mr. Levi has a broad and diverse practice that includes outsourcing transactions, technology and intellectual property licensing, fintech and blockchain matters, privacy and cybersecurity advice, branding and distribution agreements, cloud computing agreements, technology transfers, strategic alliances and joint ventures. Mr. Levi also counsels clients on website and technology policies, intellectual property strategy and regulatory compliance. His background in computer science and the information technology industry allows Mr. Levi to understand the technology and business drivers underlying transactions and agreements in these areas.

**Cristina Vasile****Tel: +1 212 735 2247 / Email: cristina.vasile@skadden.com**

Cristina Vasile is an Intellectual Property and Technology associate in Skadden's New York office. She earned her B.A. and M.A. from NYU (2008, 2009) and her J.D. from NYU School of Law (2016).

**MacKinzie Neal****Tel: +1 212 735 2856 / Email: mackinzie.neal@skadden.com**

MacKinzie Neal is an Intellectual Property and Technology associate in Skadden's New York office. She earned her B.A. from the University of Pennsylvania (2014) and J.D. from Penn Law School (2019).

Skadden, Arps, Slate, Meagher & Flom LLP

One Manhattan West, New York, New York 10001, USA

Tel: +1 212 735 3000 / URL: www.skadden.com

Distributed ledger technology as a tool for streamlining transactions

Douglas Landy, James Kong & Jonathan Edwards
Milbank LLP

This chapter will provide a high-level overview of the potential applicability of distributed ledger technology (“DLT”) to the transfer of assets represented by “tokens” or other digital assets¹ (which, for the purposes of this chapter, we will call “Transfer Tokens”), and the regulatory environment developing around such tokens. Using a token as a means of representing an underlying asset (colloquially referred to as the “tokenization” of that asset) in order to facilitate transfers of that asset is a relatively new idea, but has its roots in a very old and well-understood principle: some things that have value are not easily transferred. Whether due to practical difficulties, regulatory hurdles or imperfect or outdated trading infrastructures, sometimes the easiest way to transfer an asset – whether it be title, an ownership interest, an entitlement, or a beneficial interest in that asset – is by transferring something that represents the asset.²

Tokenization has potentially wide applicability to traditional markets. The trading of securities in the United States, for example, is beset with inefficiencies related to existing trading infrastructures. For example, purchases and sales of securities generally involve transfers of ownership that are recorded on the books of a clearing bank or the Fedwire Securities Service. Recording these transfers takes time and relies on a central intermediary. Using Transfer Tokens to represent the underlying securities can potentially streamline this process, as parties could instead exchange Transfer Tokens (and have such a transaction be reflected in a distributed ledger) that represent an interest in the securities, rather than the securities themselves.

Of course, tokenization in this manner faces a number of regulatory hurdles – some inherent to the concept itself, and some particular to each specific implementation. For example, as a general matter, it is of particular import that parties do not run afoul of the broad reach of the U.S. securities laws.³ A particular challenge is the essential dependence of many securities law analyses on the facts and circumstances of each case, precluding a one-size-fits-all approach to compliance: for example, a Transfer Token may well be considered a “security” based on a certain implementation of the concept, but not on others. Additionally, applying a layer of tokenization to traditional activities or transactions raises the broader question of whether regulation should be “technology neutral,” and whether well-established legal and regulatory regimes applicable to traditional assets or transactions must (or should be) adapted to account for the development of new technologies such as DLT and tokenization. The first section of this chapter will provide a basic overview of DLT and how it can be used to create Transfer Tokens that represent underlying assets. The second section describes a “generic” implementation of a Transfer Token, and discusses how we believe a hypothetical implementation of such a token should be characterized for the purposes of U.S. securities laws. The third section will provide two examples of potential uses of Transfer Tokens,

along with an overview of certain legal issues germane to each implementation. Finally, the fourth section reviews certain regulatory developments that have begun to shed light on how DLT and similar technologies may fit into existing legal and regulatory frameworks.

Background

While a full overview of DLT is outside the scope of this chapter, DLT (commonly implemented in the form of “blockchain” technology) generally refers to a “decentralized peer-to-peer network that maintains a ledger of transactions that utilizes cryptographic tools to maintain the integrity of transactions and some method of protocol-wide consensus to maintain the integrity of the ledger itself.”⁴ While early implementations of DLT, such as bitcoin, were limited in scope and intended primarily to facilitate peer-to-peer transfers of value, other implementations of DLT incorporate the ability for parties to “structure and update data on a ledger through robust computer code, known as smart contracts.”⁵ This allows “any asset or thing [to] be modeled on a ledger,” and “parties to run computer functions to interact with the data structures on the ledger.”⁶

One potential application of DLT in this context is the ability to “tokenize” a broad range of traditional assets, which, at least theoretically, can encompass nearly anything. In this way, transfers of the asset “can be tracked automatically on a blockchain platform in the same manner as a cryptocurrency such as Bitcoin is tracked using the same technology.”⁷ By tokenizing an asset and allowing it to be digitally represented on a blockchain or other form of distributed ledger, the process of recording and transferring ownership of the asset can be significantly streamlined. The question of whether such digital assets are “securities” is a critical one, as the application of the securities laws to the issuance and transfer of digital assets such as the Transfer Tokens could impose onerous, and potentially irrational, requirements on the “issuers” of the Transfer Tokens and hamper the ability of secondary market participants to trade Transfer Tokens amongst each other.

Characterization of tokens under securities laws

Background of treatment of digital assets

Beginning in 2017, the SEC has, through various avenues, articulated its general stance toward the regulatory classification and treatment of digital assets. In April 2019, the SEC issued its *Framework for “Investment Contract” Analysis of Digital Assets* (the “SEC Framework”). As described in the SEC Framework, any person “engaging in the offer, sale, or distribution of a digital asset” must “consider whether the U.S. federal securities laws apply,” and a threshold issue is “whether the digital asset is a ‘security’ under those laws.”⁸ While the framework is new, its essential underpinning is not: central to the SEC’s analysis has been, and continues to be, the well-worn, three-prong test articulated by the Supreme Court in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946) (“*Howey*”). The *Howey* test “applies to any contract, scheme, or transaction, regardless of whether it has any of the characteristics of typical securities,” and is meant to determine whether a particular asset or arrangement is an “investment contract” (and therefore a security). Under the test established in *Howey*, an “investment contract” exists if there is (i) an investment of money, (ii) in a common enterprise, (iii) with a reasonable expectation of profits derived predominantly from the efforts of others.

In analyzing whether something is a security, “form should be disregarded for substance.”⁹ The SEC has primarily applied the *Howey* test to digital assets because such assets do not otherwise fall into any of the enumerated categories of the definition of “security.”

Accordingly, the *Howey* test focuses not only on the form and terms of the asset or arrangement itself, “but also on the circumstances surrounding the digital asset and the manner in which it is offered, sold, or resold (which includes secondary market sales).”¹⁰ As a result, the question of whether a hypothetical Transfer Token is a “security” is one that resists blanket classification, and that instead depends on both the form and function of the Transfer Token as well as the particular facts and circumstances surrounding the issuance, offering, and secondary market transfers of the Transfer Token.

While “[no] one factor is necessarily dispositive as to whether or not an investment contract exists,”¹¹ the SEC Framework articulates a wide range of factors that would be indicative of the presence of an “investment contract,” mapping these factors to each prong of the *Howey* test. These factors include, among others:

- An investment of money: Investors purchase or otherwise acquire the digital asset in exchange for value, whether that value takes the form of fiat currency, another digital asset, or another type of consideration.
- A common enterprise: While the SEC Framework notes that the SEC does not view the “common enterprise” requirement as a distinct element of the *Howey* test, the SEC noted that investments in digital assets have generally constituted investments in a common enterprise “because the fortunes of digital asset purchasers have been linked to each other or to the success of the promoter’s efforts.”¹²
- Reasonable expectation of profits derived from efforts of others: An investor has a reasonable expectation of profits derived from the efforts of others if a promoter, sponsor, or other third party (each, an “Active Participant” or “AP”) provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profit from those efforts. While no one factor is determinative, the SEC Framework lists the following factors as indicative of whether this prong is met:
 - the purchaser reasonably expects to rely on the efforts of an AP;
 - the managerial efforts are significant and affect the failure or success of the enterprise, as opposed to efforts that are ministerial in nature;
 - an AP is responsible for the development, improvement, operation, or promotion of the network;
 - where the network or digital asset is still in development or not yet fully functional, investors would reasonably expect an AP to further develop the functionality of the network and/or digital asset;
 - there are essential tasks or responsibilities performed and expected to be performed by an AP;
 - an AP creates or supports a market for, or the price of, the digital asset;
 - an AP has a lead or central role in the direction of the ongoing development or management of the network or the digital asset;
 - investors would reasonably expect the AP to undertake efforts to promote its own interests and enhance the value of the network or digital asset, such as where the AP has the ability to realize capital appreciation from the value of the digital asset, the AP distributes the digital asset as compensation to management, or the AP monetizes the value of the digital asset;
 - the digital asset gives the holder rights to share in the enterprise’s income or profits or to realize gain from capital appreciation of the digital asset;
 - the digital asset is transferable or traded on a secondary market or platform;
 - purchasers reasonably would expect the AP’s efforts to result in capital appreciation of the digital asset;

- the digital asset is offered broadly to potential purchasers or in quantities indicative of investment intent;
- the AP is able to benefit from its efforts as a result of holding the same class of digital assets as those being distributed to the public;
- the potential profitability of the operations of the network or the potential appreciation in the value of the digital asset is emphasized in marketing or other promotional materials; and
- the availability of a market for the trading of the digital asset.

In contrast, the SEC Framework highlights a number of factors that, while not necessarily determinative, would support the notion that the *Howey* test is not met,¹³ including:

- the distributed ledger network and digital asset are fully developed and operational;
- holders of the digital asset are immediately able to use it for its intended functionality on the network;
- the digital assets' creation and structure is designed and implemented to meet the needs of its users, rather than to feed speculation as to its value or development of its network;
- prospects for appreciation in the value of the digital asset are limited;
- any economic benefit that may be derived from appreciation in the value of the digital asset is incidental to obtaining the right to use it for its intended functionality;
- the digital asset is marketed in a manner that emphasizes its functionality rather than the potential for the increase in market value of the digital asset;
- potential purchasers have the ability to use the network and the digital asset for its intended functionality;
- restrictions on the transferability of the digital asset are consistent with the asset's use and not facilitating a speculative market; and
- if the AP facilitates the creation of a secondary market, transfers of the digital asset may only be made by and among users of the platform.

Application of the securities laws and the SEC Framework to Transfer Tokens

As noted above, the question of whether the Transfer Token is a “security” depends on both the form and function of the Transfer Token as well as the particular facts and circumstances surrounding the issuance, offering, and secondary market transfers of the Transfer Token. Provided the aim is to design a Transfer Token such that (i) the hallmarks of a “security” described in the SEC Framework are generally not present, in either form or substance, and (ii) the factors that would indicate that a digital asset is *not* a security *are* present, we imagine a generic Transfer Token with a number of essential characteristics that we believe should, when analyzed through the prism of the factors articulated by the SEC above, cause that Transfer Token to fall outside the definition of security. These characteristics include:

- The Transfer Tokens are issued to represent a specific underlying asset, and are designed for the express purpose of facilitating a transfer of that asset.

Discussion: In general, the more narrowly tailored the design of the Transfer Token, the less likely it would be to fall under the auspices of the securities laws. For example, in a hypothetical implementation, a holder of a Transfer Token (a “Token Holder”) may deposit assets, such as cash or securities, with a custodian, and receive Transfer Tokens representing said cash or securities in return.¹⁴ The Transfer Tokens could then be used to facilitate transfers of the underlying cash or securities to other market participants who maintain accounts at that custodian. Recipients of Transfer Tokens could, in turn, “redeem” the Transfer Tokens with the custodian in order to receive the underlying cash or securities. Under this model, the Transfer Tokens' creation and use – tied solely to facilitating a transfer of the underlying assets – would more likely be considered to have been designed and structured to meet the needs of users, rather than to feed speculation.

- Note that, given the SEC’s broad interpretation of an “investment” of money under the *Howey* test, such an acquirer of Transfer Tokens may nevertheless be considered to be making an “investment” of value. However, the acquirer is not obtaining the Transfer Tokens for investment *purposes*; rather, the acquirer is *exchanging* some form of property for a Transfer Token that represents that property, and subsequently using the resulting Transfer Token to effect a transfer of that property to another party. Crucially, the Transfer Token itself is not purchased because of its value; rather, the Transfer Token should be envisioned as having no value in and of itself, and more akin to a book-entry representing some underlying asset rather than an asset itself.¹⁵

- Because Transfer Tokens are created to represent specific underlying assets and have no value distinct from those assets, there is no “common enterprise” linking the fortunes of the entity issuing Transfer Tokens to Token Holders, or the fortunes of Token Holders to each other.

Discussion: While the SEC “does [not] view a ‘common enterprise’ as a distinct element of the term ‘investment contract,’” the SEC Framework notes that “investments in digital assets have constituted investments in a common enterprise because the fortunes of digital asset purchasers have been linked to each other or to the success of the promoter’s efforts.” In particular, the SEC Framework notes that investors in a digital asset that is a security would reasonably expect capital appreciation in the value of the digital asset based on the efforts of an AP. This is not the case with respect to the Transfer Tokens; Token Holders’ fortunes are neither linked to the fortune of the “issuer” of the token nor to the fortunes of other Token Holders. Rather, Token Holders’ fortunes are tied only to the value of the underlying asset represented by the Transfer Token, whose value should not be affected by the tokenization of the asset.

- Additionally, because Transfer Tokens are tied to specific underlying assets and designed to facilitate a transfer of those assets, market participants would not acquire the *tokens themselves* with a reasonable expectation of profits predominantly from the efforts of others.

Discussion: In contrast to scenarios described in the SEC Framework, there is no AP in the transactions imagined in this chapter that would retain the digital asset, or that would support the price of the digital asset, undertake efforts to enhance the value of the digital asset, or have the ability to realize capital appreciation from the value of the digital asset. The Transfer Tokens are created merely to streamline the process by which market participants may transact in certain types of assets and transfer interests among each other. Participants acquire Transfer Tokens not to profit from the efforts of others, but to more easily effectuate the envisaged transaction(s) in the underlying asset.

- The Transfer Tokens imagined would be issued on a functioning network, be designed to replicate and streamline the process normally associated with transacting in the asset represented, and be distributed only among people or institutions that comprise the existing market for the underlying asset.

Discussion: As noted above, the *Howey* test is less likely to be met if a digital asset’s creation and structure is designed and implemented to meet the needs of its users and the restrictions on the transferability of the digital asset are consistent with the asset’s use. This would generally mean, for example, that to the extent that purchasers of an underlying asset would be limited to individuals or institutions that meet certain criteria, the issuance and transfer of Transfer Tokens should also be so limited.

- Because the Transfer Tokens are meant to replicate “traditional” interests in the underlying assets represented by the Transfer Tokens, one of the primary policy

purposes of the securities laws articulated by the SEC – *i.e.*, compelling disclosure in order to reduce informational asymmetries between promoters and investors – would be inapplicable to the use of Transfer Tokens imagined by this chapter, because no informational asymmetry is produced by the tokenization of an asset. No part of the “traditional” transaction in the asset is in substance altered by tokenization, and as noted above, the creation of Transfer Tokens can be more properly envisioned as the creation of an electronic book-entry representing an underlying asset, rather than the creation of a new asset itself.

Potential applications of Transfer Tokens

Within the model articulated in the foregoing section, Transfer Tokens may be used to streamline transactions in a potentially wide range of assets, although different legal considerations may apply to each. This section reviews the potential applicability of Transfer Tokens to two distinct markets, the syndicated loan market and the market for artwork, and briefly discusses certain relevant considerations with respect to each.

Syndicated loans

Syndicated term loans are traded by a range of sophisticated financial institutions, including commercial banks, investment banks, hedge funds, broker-dealers, and other institutions. One potential application of DLT using Transfer Tokens involves “tokenizing” an interest in a syndicated loan that has been purchased by a lender or secondary market participant pursuant to an assignment or participation. In this way, “[t]he loans held by lenders in a syndicate can be tracked automatically on a blockchain platform in the same manner as a cryptocurrency such as Bitcoin is tracked using the same technology.”¹⁶ By tokenizing an asset and allowing it to be digitally represented on a blockchain or other form of distributed ledger, the process of recording and transferring ownership of the asset should be significantly streamlined.

The syndicated loan market is perhaps an ideal candidate for the application of DLT: loans are currently originated (and trades conducted) pursuant to a complicated suite of documentation, which can theoretically be simplified and made more transparent by reflecting the essential terms of such documentation on a blockchain. Additionally, the underlying assets – loan interests – are generally not considered securities, and so the trading of loan interests among financial institutions has not been considered subject to the securities laws.¹⁷ The tokenization of loan interests, then, should not be considered to jeopardize that characterization, *provided* that the tokenization is designed solely to facilitate efficient transfer and record-keeping with respect to secondary market transactions in the interests.

For example, a Transfer Token should be designed such that a Token Holder would own an assignment or participation interest in a syndicated term loan in the same manner as the holder of a “traditional” assignment or participation interest, and the rights and obligations of that Token Holder would likewise be identical to that of a lender purchasing a traditional assignment or participation interest. Furthermore, such Transfer Tokens should be subject to certain restrictions on transfer, such that they could be traded only among the same sophisticated financial institutions that currently participate in the secondary market for loans, and transfer should be subject to the same restrictions (*e.g.*, the consent of the borrower) that currently apply to the sale and transfer of loan interests. Lastly, we would expect that the Tokens would be issued by the originating financial institutions (or affiliates thereof), transferred through a fully functioning private or public blockchain (which may be developed, operated,

and/or maintained by the financial institutions originating or participating in the loan), and would not be made freely available to the public on a secondary market trading platform in a manner inconsistent with the current marketing and sale process applicable to syndicated loans. Such a design should, consistent with the objectives discussed above, minimize the hallmarks of a “security” described in the SEC Framework.

Notwithstanding the foregoing, the *Howey* test *may* be met if the Tokens possessed additional characteristics inconsistent with traditional limitations on the marketing and sale of loan interests. For example, if the Tokens were to be freely tradeable on a secondary market platform among the public or participants who did not have the ability to request information from, or conduct due diligence on, the borrower, such transferability would implicate certain of the important policy considerations of the securities laws and may cause the Tokens to be considered securities. As always, the facts and circumstances are crucial.

Artwork

One perhaps novel use of Transfer Tokens envisioned under this framework would be for transfer of artwork. Transacting in certain types of property under American law can be a complicated exercise, and artwork falls into a category of property that faces certain practical obstacles to transfer. Contemporary art transfers typically involve a trusted intermediary (such as an art dealer or gallery) who agrees to store and present the artwork to potential buyers for a hefty fee.¹⁸ At the same time, these traditional intermediaries offer a necessary legitimizing function, whether it is in reviewing art pieces for authenticity, evaluating the quality of art presented and sold, or collecting artwork under a centralized clearinghouse which makes it easier for art buyers and sellers to find the pieces they want. As a result, traditional intermediaries create markets for art transactions that otherwise would not exist.

DLT could be used to create more efficient artwork markets. For example, a company dedicated to compiling registries for unique assets recently partnered with a start-up company to auction digital and physical artworks associated with what could be characterized as Transfer Tokens on the Ethereum blockchain platform, with each Transfer Token associated with a unique piece of art.¹⁹ Based on the early success of DLT-facilitated artwork transfers, traditional art houses and galleries have reportedly started experimenting with auctions using blockchain technology to move artwork between interested parties.²⁰ The benefits of publicly verifiable and secure digital transactions in the art space can be echoed across industries, and the success of DLT as applied to artwork might trigger other innovative uses of Transfer Tokens for other difficult-to-transfer goods.²¹

Regulatory developments

The use of Transfer Tokens, and the advent of new financial technologies more broadly, raises the fundamental question of how assets, activities or transactions that are subject to well-established legal and regulatory regimes should be treated when superimposed with the overlay of new technology. On the one hand, institutions that employ solutions such as DLT in an effort to streamline existing activities or processes, or that propose to conduct traditional activities (such as providing bank custody services) but with respect to assets such as digital tokens, could be viewed as engaging in the same activities that have always been permissible to them. On the other hand, the use of novel technology could potentially introduce new risks to existing activities, or even alter the essential nature of the underlying activity in ways that warrant additional scrutiny.

While there is unlikely to be a universal answer to this question, recent years have provided some indication of how regulators are beginning to grapple with these issues. Perhaps the

issue that has received the most attention is the question of whether digital assets should be considered “securities” subject to the securities laws, as discussed under “Characterization of tokens under securities laws” above. In this area, the SEC has made clear that substance, as analyzed against longstanding precedent, should prevail over form. While the SEC Framework dates to 2019, it fundamentally represents an attempt by the SEC to apply the well-trod principles set forth in *Howey*, a court case decided in 1946, to the particular qualities germane to digital assets.

While many of the SEC’s most visible activities in the digital asset realm have taken the form of enforcement actions against entities conducting unregistered securities offerings, the agency has also shown a willingness to encourage DLT-based market innovation. In testimony before the U.S. Senate in 2019, SEC Chairman Jay Clayton stated that he was “optimistic that developments in distributed ledger technology can help facilitate capital formation, providing promising investment opportunities for both institutional and Main Street investors,” adding that he believed the SEC has taken a “measured, yet proactive regulatory approach that both fosters innovation and capital formation while protecting our investors and our markets.”²² In October of 2019, the SEC issued a no-action letter to Paxos Trust Company, LLC (“Paxos”) allowing Paxos to conduct a time-limited “feasibility study” involving the use of DLT to facilitate the clearance and settlement of listed U.S. equity securities trades in a production environment involving several large broker-dealers.²³ While a full review of the settlement service offered by Paxos is outside the scope of this chapter, the system bears a number of similarities to the Transfer Tokens described herein: participants in the Paxos system may deposit eligible cash or securities into a settlement account and receive digitized security entitlements in return, which may be used to facilitate the settlement of transactions involving the purchase or sale of such deposited securities. While the SEC’s no-action letter to Paxos is strictly limited to the SEC’s enforcement stance and declines to address the substance of Paxos’ legal conclusions, the letter is a potential indication that the SEC may be receptive to the viability of Transfer Tokens and their use to facilitate securities settlement.²⁴

In July 2020, the Office of the Comptroller of the Currency (the “OCC”) issued an interpretive letter confirming the authority of a national bank to provide cryptocurrency custody services for customers, provided that the bank effectively manages the risks and complies with applicable law.²⁵ Notably, the interpretive letter cited national banks’ longstanding authority to provide “safekeeping and custody services for a wide variety of customer assets,” and added that such functions were “well established and extensively recognized as permissible activities for national banks.”²⁶ In concluding that providing cryptocurrency custody services “is a modern form of these traditional bank activities,” the letter went on to note that “as the financial markets become increasingly technological, there will likely be increasing need for banks...to leverage new technology and innovative ways to provide traditional services on behalf of customers.”²⁷ In September 2020, the OCC issued an additional interpretive letter confirming the authority of national banks to provide banking services to cryptocurrency businesses and to receive deposits from issuers of “stablecoins,” including deposits that constitute reserves for a stablecoin that is backed on a 1:1 basis by underlying fiat currency.²⁸ As was the case under the previous interpretive letter, the OCC found that providing such services constituted core banking activities that national banks are free to engage in, subject to effective risk management and compliance with applicable law. Both interpretive letters echoed sentiments expressed by the OCC in an Advance Notice of Proposed Rulemaking (“ANPR”) issued in June 2020, in which the OCC stated that it has “long understood that the banking business is

not frozen in time and agrees with the statement made over forty years ago by the U.S. Court of Appeals for the Ninth Circuit: “the powers of national banks must be construed so as to permit the use of new ways of conducting the very old business of banking.”²⁹ At the same time, the ANPR acknowledged that technological changes presented both opportunities and “new challenges and risks,” and asked for comment regarding whether certain aspects of the existing bank regulatory framework should be revised to reflect technological advances and innovations. Taken together with the SEC’s recent statements, the OCC pronouncements reinforce the notion that regulators will likely be willing to embrace technological innovation so long as it is conducted in a sound, responsible manner with an eye toward mitigating any attendant risks.

Conclusion

Transfer Tokens offer a wide range of possibilities when it comes to streamlining transactions in traditional assets. As reviewed herein, there are strong arguments that the model Transfer Tokens described in this chapter are not securities (or even, in themselves, assets), and that tokenizing an asset to facilitate its transfer should not change the legal or economic substance of the transaction. While the potential applicability of Transfer Tokens is vast, however, market participants must carefully review each implementation – especially when evolving, highly regulated financial markets are involved – to ensure that the attendant legal issues are properly addressed.

* * *

Endnotes

1. It should be noted that the use of the term “digital assets” is somewhat of a misnomer, as assets are typically understood as things that have value. Ideally, the Transfer Token should be conceptualized as akin to a book-entry that has no value in and of itself, but merely represents an underlying asset. Even the use of the word “token” is problematic, as it can both imply value and carry negative connotations associated with the raft of tokens issued pursuant to “initial coin offerings” in recent years. Here, we use the word token to mean that it is *symbolic*.
2. One archetypal example of this concept drawn from traditional markets, of course, is the framework that has developed around the indirect ownership of securities under the Uniform Commercial Code (“UCC”). In response to a “paperwork crisis” on Wall Street during the 1960s and 1970s, when the burden of reconciling trades using the traditional certificate-based system overwhelmed brokerage firms and transfer agents, the Depository Trust Company (“DTC”) was created to act as a central securities depository and hold immobilized share certificates on behalf of its participants. The regulatory scheme that governs transfers of interests in the securities held by DTC is Article 8 of the UCC, which provides that persons holding securities through brokers or custodians hold “security entitlements,” rather than direct ownership of the underlying securities. Article 8 describes the package of rights held by the holder of a security entitlement (the “entitlement holder”), and provides that an entitlement holder may issue an “entitlement order” in respect of a financial asset that directs an intermediary to transfer or redeem the financial asset to which the entitlement holder has a security entitlement.
3. The use of “securities laws” in this chapter generally refers to the Securities Act of 1933 (the “Securities Act”) together with the Securities Exchange Act of 1934 (“Exchange Act”) and the regulations and interpretations issued thereunder.

4. See *Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part One: Generation Considerations and Blockchain Primer*, LSTA (2018).
5. *Id.*
6. *Id.*
7. See *Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part Three: Application of Blockchain Technology to the Loan Market*, LSTA (2018).
8. SEC Framework, Section I.
9. *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967).
10. *Id.*
11. SEC Framework, footnote 4.
12. SEC Framework, footnote 11.
13. The SEC issued, concurrently with the SEC Framework, a no-action letter addressed to an air charter service company proposing to issue “blockchain-based digital assets in the form of ‘tokenized’ jet cards.” In that letter, the SEC stated that it would not recommend enforcement against the company for issuing tokens without registration under the securities laws, because (i) the company would not use the proceeds from its token sale to develop a platform or network, which would be fully developed and operational by the time any tokens were sold, (ii) the tokens would be immediately usable for their intended functionality (*i.e.*, purchasing air charter services) at the time of the sale, (iii) transfers of the tokens would be restricted to the company’s wallets, (iv) tokens would be sold at one USD per token throughout the life of the program, and each token represented an obligation by the company to supply air charter services at a value of one USD per token, (v) the company would only offer to repurchase tokens at a discount to their face value, and (vi) the tokens would be marketed in a manner that would emphasize their functionality, rather than the potential for increase in its market value. See <https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm>. On July 25, 2019, the SEC issued a second no-action letter to a gaming platform operator that proposed to sell “Quarters” to gamers for use in online video games. In that letter, the SEC noted the presence of factors similar to those cited in its previous letter, including that the platform would be fully operational immediately upon its launch (and before the sale of any Quarters), that Quarters would be immediately usable for their intended purpose and transferable only among other wallets on the platform, that Quarters would be made continuously available at a fixed price, and that Quarters would be sold solely for consumptive use as a means of accessing and interacting with participating games. See <https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1>.
14. A custodian, for these purposes, would be a financial institution licensed or chartered to provide custodial services. However, the token *issuer* may (but is not necessarily required to be) the custodian itself; for example, we envision that token issuances and redemptions may be handled by a third-party company or by a platform maintained and operated by a consortium of institutions. While we generally do not believe the identity of the token issuer should, in itself, alter the analysis or whether the issued tokens are securities, additional analysis may be required regarding whether the activities of such a company or platform would cause it to fall within the definition of a “clearing agency” subject to registration with the SEC, and if so, whether an exemption from registration would be available.

15. The model Transfer Tokens described in this chapter are distinguishable from cryptocurrencies that are purchased because of their value and that are not typically representative of any underlying asset. Such cryptocurrencies do often bear the hallmarks of investment vehicles. The proposed Libra cryptocurrency, however, broke with the more traditional formulation of blockchain-based cryptocurrencies when it was first introduced in 2019, because it would be backed by a reserve of low-volatility assets, which the creators called the Libra Reserve. While a full discussion of the Libra is beyond the scope of this chapter, Libra, as envisioned by its creators, could be a new type of cryptocurrency with the potential to bring access to low-cost means of transferring money to those who currently have little or no access to financial services. In order to be successful, the creators of the Libra note that it must be more widely adopted than other cryptocurrencies have been to date, citing volatility as one of the major impediments to adoption. In order to alleviate the volatility often associated with blockchain-based cryptocurrencies, Libra would be backed by assets like bank deposits and short-term government securities. Because of this, the Libra could be errantly described as being representative of the assets that support its value. However, the assets that make up the reserve can be viewed more accurately as a tool to decrease volatility and thereby increase potential adoption. The Libra *itself* is intended to have value, and the underlying assets are intended to provide a stable range to that value. Therefore, despite the apparent similarity between a formulation of Libra backed by low-volatility assets and the Transfer Tokens proposed by this chapter that are representative of assets having value, the two concepts differ in a way that is crucial to the analysis of the applicability of securities law: the former is intended to have value in and of itself; and the latter is intended to be merely representative of an underlying valuable asset with no intrinsic value of its own. See <https://libra.org/en-US/white-paper/>. Libra's 2019 proposal received significant regulatory and legislative pushback from U.S. and foreign governments, and in 2020, the Libra Association announced that it would modify its proposal to introduce single-currency stablecoins backed by individual national currencies. See <https://libra.org/en-US/updates/finma-payment-system-license/>. As of this writing in September 2020, Libra has yet to be launched.
16. See *Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part Three: Application of Blockchain Technology to the Loan Market*, LSTA (2018).
17. See *Banco Espanol de Credito v. Security Pac. Nat'l Bank*, 973 F.2d 51 (2d Cir. 1992).
18. See "How to Approach Selling Art as a Collector," Artwork Archive (2019), available at <https://www.artworkarchive.com/blog/how-to-approach-selling-art-as-a-collector>.
19. See R. O'Dywer, "A Celestial Cyberdimension: Art Tokens and the Artwork as Derivative," *Circa Art Magazine* (accessed July 21, 2019), available at <https://circaartmagazine.net/a-celestial-cyberdimension-art-tokens-and-the-artwork-as-derivative/>.
20. H. Neuendorf, "Christie's Will Become the First Major Auction House to Use Blockchain in a Sale," ArtNet News (2018), available at <https://news.artnet.com/market/christies-artory-blockchain-pilot-1370788>.
21. See "Blockchain in Oil & Gas," Deloitte (accessed July 21, 2019), available at <https://www2.deloitte.com/us/en/pages/consulting/articles/blockchain-digital-oil-and-gas.html>.
22. See Testimony on "Oversight of the Securities and Exchange Commission" Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, available at <https://www.sec.gov/news/testimony/testimony-clayton-2019-12-10> (Dec. 10, 2019).

23. See Letter from Jeffrey S. Mooney, Associate Director, SEC, to Charles G. Cascarilla & Daniel M. Burstein, Paxos Trust Company, LLC, *available at* <https://www.sec.gov/divisions/marketreg/mr-noaction/2019/paxos-trust-company-102819-17a.pdf> (Oct. 28, 2019).
24. On September 25, 2020, the SEC issued a no-action letter permitting registered broker-dealers that meet certain requirements to operate alternative trading systems (“ATS”) that trade digital asset securities, provided the ATS is organized such that: (i) a buyer and seller send their respective orders to the ATS, notify their respective custodians of such orders, and instruct their respective custodians to settle transactions in accordance with the terms of their orders when the ATS notifies the custodians of a match on the ATS; (ii) the ATS matches the orders; and (iii) the ATS notifies the buyer and seller of their respective custodians of the matched trade, upon which the custodians would settle the trade on behalf of the buyer and seller. See Letter from Elizabeth Baird, Deputy Director, Division of Trading and Markets, SEC, to Kris Dailey, Financial Industry Regulatory Authority, *available at* <https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf> (Sept. 25, 2020).
25. See Interpretive Letter #1170, OCC, *available at* <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf> (July 2020).
26. *Id.*
27. *Id.*
28. See Interpretive Letter #1172, OCC, *available at* <https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf> (Sept. 21, 2020). On September 21, 2020, SEC staff issued a statement regarding this OCC interpretive letter, emphasizing that the question of whether a particular digital asset (including a stablecoin) is a security under the federal securities laws is inherently a facts and circumstances determination. The SEC statement is *available at* <https://www.sec.gov/news/public-statement/sec-finhub-statement-occ-interpretation>.
29. See *National Bank and Federal Savings Association Digital Activities*, Advance notice of proposed rulemaking, *available at* <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-76a.pdf>.

**Douglas Landy****Tel: +1 212 530 5234 / Email: dlandy@milbank.com**

Milbank partner Douglas Landy, an expert in US financial services regulation and financial technology issues, is noted for his deep experience in banking and financial technology laws and has published numerous related articles and spoken on related issues. With particular expertise in cybersecurity and financial technology matters, the Volcker Rule, capital requirements, bank insolvency laws, and US-based foreign bank operations, he is widely sought after by clients, representing many of the leading global banks and central counterparties in matters in front of federal and state regulatory agencies. Select highlights include advising: the State of Wyoming on amending banking and UCC laws to encourage Bitcoin/cryptocurrency transactions; Digital Asset in a groundbreaking legal review of a proposed new blockchain product; a multinational bank on a transfer of material business information to cloud services worldwide; a global bank on cyber privacy work; and ongoing regulatory and supervisory issues raised by financial services regulators with respect to technology innovations.

**James Kong****Tel: +1 212 530 5244 / Email: jkong@milbank.com**

James Kong, a senior associate at Milbank, is highly experienced in bank regulatory, cybersecurity and financial technology matters. Mr. Kong has provided counsel to US and foreign financial institutions on a diverse range of regulatory and compliance matters, including with respect to the US Bank Holding Company Act, the Volcker Rule and other aspects of the Dodd-Frank Act, regulatory expectations regarding vendor risk management and third-party relationships, and anti-money laundering laws and regulations. Select highlights of his recent financial technology work includes advising: the State of Wyoming in its drafting of legislation that would provide legal clarity to financial institutions seeking to custody or secure interests in digital assets; Digital Asset in a groundbreaking legal review of a proposed new blockchain product; a multinational bank on a “first in industry” transfer of material business information from internal data storage facilities to third-party cloud service providers; and a global bank on the Volcker Rule and cybersecurity and data privacy work.

**Jonathan Edwards****Tel: +1 212 530 5476 / Email: jedwards2@milbank.com**

Jonathan Edwards, an associate at Milbank, represents banks and other financial institutions in a broad range of domestic and international financing transactions and financial technology matters. He has worked for a variety of clients on matters involving acquisition financings, first and second lien financings and other secured and unsecured lending transactions. Jonathan co-authored a chapter on “Regulation and Compliance in a Blockchain World” in *Blockchain in Financial Markets and Beyond: Challenges and Applications*, and co-authored recent client alerts titled “Bitcoin and the Volcker Rule: Are Banks Banned from Cashing in on the Crypto Craze?” and “Part 2 – Blockchain and the Volcker Rule: Are Cryptocurrency Companies Covered Funds?”.

Milbank LLP

55 Hudson Yards, New York, NY 10001-2163, USA

Tel: +1 212 530 5000 / Fax: +1 212 530 5219 / URL: www.milbank.com

Blockchain M&A: The next link in the chain

An overview of key drivers and unique valuation, due diligence, and integration hurdles for the current wave of blockchain M&A

F. Dario de Martino
Morrison & Foerster LLP

Despite having experienced the “crypto winter” and being in the middle of a rare combination of public health, political, social, and economic uncertainties plaguing the global business landscape, blockchain market participants have remained steadfast and are continuing to ride the wave of M&A.¹

While most transactions in this space are private, and their terms are confidential or otherwise not material enough to be publicly disclosed, the data available indicates that there have been approximately 400 blockchain-related M&A transactions globally since 2013, with about 40 in the first half of 2020, for a total estimated value of approximately \$5 billion.²

If current deal flow holds steady, blockchain M&A will likely match or exceed the deal volume levels of 2019 at valuations that have already come close to, or exceeded, those of 2019, illustrating the industry’s resilience.

In this age of remote work with no clear silver lining in sight, businesses will likely be looking farther afield for enterprise technologies that facilitate remote trading, collaboration among disparate stakeholders, network decentralisation, and data securitisation – preferably all in one service package. Moreover, as they grow more comfortable with digital assets³ and blockchain more generally, larger public institutions and their investors may find that a diverse industry still largely composed of startups makes for an increasingly attractive environment for deal-making.

As blockchain technology continues to mature, digital assets shine in their hedging role against the many current uncertainties, and regulatory frameworks evolve towards establishing more discernible parameters, we believe there is enough stability to support blockchain M&A, including cross-border M&A, through the end of the year and beyond.

Key drivers of blockchain M&A

In addition to a desire to drive growth, diversify the range of existing blockchain-related offerings, or pivot toward new business lines, many blockchain M&A transactions are being pursued to gain access to skilled talent as well as address a rapidly evolving regulation of digital assets.

Driving growth

After the whipsaw frenzy of 2017, the lustre faded and crypto winter washed out those companies unprepared for longer-term stabilisation. Many of the companies that weathered the storm have favoured M&A as a growth driver.

For example, despite a regulatory framework in flux, Coinbase has thrived and expanded through 16 acquisitions across diverse industries, from digital wallet services to data and

analytics application programming interface (API) development. This ingathering of different services and business solutions under a single umbrella has enabled the exchange to tap into diverse revenue streams to support its growth into arguably the largest U.S. cryptocurrency exchange, a business scaled up to handle \$500 million in trade volume daily. Other major exchanges worldwide, including Kraken and Binance, have taken similar approaches and reaped similar rewards.

Broadening the range of existing blockchain-related offerings

Despite being a nascent industry, the number of blockchain offerings available for trading and enterprise implementation is manifold. Focusing on digital assets alone, estimates suggest there are anywhere from 6,000 to 9,000 different varieties in circulation at any given time, even excluding crypto derivatives and other more sophisticated instruments.

On the one hand, this demonstrates the relatively short lifecycle of many digital assets. On the other hand, the high volume of new offerings represents a unique opportunity for companies to acquire promising blockchain technology and other intellectual property (IP) that would otherwise be cost-prohibitive to develop in-house.

Acquisitions by larger players focused on absorbing smaller startups to integrate IP and know-how into their own platform, known as “bolt-on” or “tuck-in” acquisitions, have become a key part of the playbook in blockchain M&A. For example, in November 2019, Gemini Trust Company acquired non-fungible token developer Nifty Gateway as a shortcut to developing its own native non-fungible protocols.

Pivoting toward new business lines

For most of blockchain’s history, the key players driving its development have not been legacy financial institutions or the tech giants of Silicon Valley.

The froth of the digital asset market in the run up to 2018 and the U.S. federal agencies’ subsequent crack-down spooked many high-end market participants. However, blockchain market participants have since made a concerted effort to comply with often restrictive U.S. federal rules and regulations to normalise this industry. Most significantly, vindication of the industry’s progress came this past July with the decision by the Office of the Comptroller of the Currency to allow national banks and savings associations to hold select digital assets on behalf of their clients. The greenlight for these services may finally allow legacy financial institutions to close their innovation gaps with moves into blockchain M&A.

Outside of the United States, there was some movement in this direction. In August 2018, the Japanese e-commerce giant Rakuten, Inc. acquired the crypto exchange platform Everybody’s Bitcoin for \$2.4 million. Rakuten then used that acquisition as its on-ramp for further blockchain partnerships and spot trading services through the end of 2019.

Acqui-hiring

According to a recent market analysis,⁴ the jobs that keep seeing the most demand are for software developers and engineers, and the most in-demand hard skill is blockchain.

However, while it is possible to rely on traditional hiring methods and fill key positions in this market, some companies do not have the luxury of waiting or the patience to wait to assemble a team with a hard-to-find skill set in a piecemeal fashion. Instead, market participants often find that the most expedient solution to staff a specialised team is to “acqui-hire”, *i.e.*, to acquire a company’s shares or assets primarily for its pool of talent, often software developers and engineers who are leaders in their respective areas of expertise and can fast-track the acquirer’s blockchain-enabled applications.

Facebook, for example, made headlines by acquiring Chainspace and Servicefriend in 2019; without the specialised talent influx, the ensuing development of Libra and Calibra (now Novi) may have been significantly delayed.

Regulatory-driven M&A

As is characteristic in regulated industries, there are a host of registrations, licences, no-action relief, and other approvals that may need to be obtained prior to expanding operations in new jurisdictions or rolling out a new regulated blockchain-enabled product.

As a result, both U.S. and non-U.S. market participants consider M&A a tool that enables them to attain advisory and broker-dealer capabilities, offer blockchain-enabled securities, or create an entry point to service U.S. investors seeking to participate in non-U.S. markets, or non-U.S. investors seeking to participate in the U.S. market, in each case, under the oversight of the relevant regulators.

Coinbase, for example, obtained a broker-dealer licence, an alternative trading system licence, and a registered investment adviser licence through its simultaneously announced acquisitions of Keystone Capital Corp., Venovate Marketplace, Inc., and Digital Wealth, LLC in 2018. Similarly, Kraken acquired UK-based Crypto Facilities, an entity registered with the UK's Financial Conduct Authority, which allowed Kraken to offer its customers the ability to trade digital asset derivative products beyond the United States' trading-hour limits and expand its European customer base.

Issues unique to blockchain M&A

Structuring and executing an M&A transaction in this highly competitive space can be complex. A combination of challenging valuation, due diligence, and integration hurdles has the potential to put a new spin on what would otherwise be a traditional M&A transaction. As a result, it is critical for market participants to factor into deal analysis and planning the unique issues surrounding a blockchain M&A transaction.

Valuation issues

Traditional valuation methods

Valuation of a blockchain target presents a few hurdles that require a nuanced approach.

Although an in-depth analysis of issues involving valuation of blockchain companies is beyond the scope of this chapter, at a high level, investment bankers typically summarise the range of values for a prospective target by drawing on three primary valuation methods: (i) discounted cash flow (DCF) analysis; (ii) comparable companies analysis; and (iii) comparable transactions analysis.

Under the DCF analysis method, the theoretical value of a target is the sum of the future stream of free cash flow it is expected to generate, discounted by its cost of capital. However, regardless of the current uncertainties caused by the pandemic, a DCF analysis is generally not recommended for emerging blockchain companies, for there is likely limited predictability of future cash flows and therefore it may be challenging to prepare projections that owe more to hope than reason.

A comparable companies analysis (also called “trading multiples”, “peer group analysis”, “equity comps”, or “public market multiples”) compares the target against selected, similarly situated companies by looking at multiples of each company against selected benchmarks, typically EBITDA (which is often used for established companies with earnings), and revenues (which is often used for companies that have been able to generate sales, but

have not yet reached profitability). Using trailing 12 months of EBITDA or of revenues is generally a reasonable way for acquirers to try to predict future financial performance of a prospective target. However, regardless of the current uncertainties caused by the pandemic, this method may be inadequate where it is difficult to assess actual comparability or there are not enough comparable companies in the same industry or stage of their growth cycle.

A comparable transactions analysis is similar to the comparable companies analysis, but the companies used as models are recently acquired companies. However, this method may also be inadequate where there are simply not enough comparables in the data set.

As noted above, most transactions in this space are private, and their terms have been kept confidential or are otherwise not material enough to be publicly disclosed; in addition, only a few blockchain targets are public. Therefore, none of the traditional comparable valuation methods may be adequate, helpful, or reliable.

Alternative valuation methods

When traditional avenues of valuation are unreliable, market participants may consider other analyses or metrics. For example, employing the “build v. buy” analysis, under which an acquirer would evaluate the cost and time required to build the target’s technology stack in-house, *versus* the cost and time to buy the target and employ its skilled employees.

To make things more interesting, several blockchain targets have developed, or in some cases are still developing, novel technologies that are not proven or have not yet been commercialised on a large scale; therefore, a much deeper dive into the underlying technology stack is required. Blockchain, in and of itself, is an umbrella term used to describe a variety of technologies that typically include distributed ledgers, cryptography, and smart contracts. As noted above, the expertise required to evaluate each of these technologies, including, for example, the scalability requirements of a given blockchain-enabled platform, how they interact with one another, or how they could be integrated, is a scarce commodity, and in some cases, finding a pool of talent with the right skill set is the main driver of an acquisition in this space, which makes this process challenging, and potentially quite circular.

Acquiring a blockchain target that also holds digital assets, or paying part or all of the consideration for a target with digital assets, presents additional challenges.

Again, although an in-depth analysis of issues involving valuation of digital assets, including the effects of volatility, market manipulation, forks, and drops, is beyond the scope of this chapter, at a high level, it is worth noting that, unlike traditional debt and equity securities or commodities, there is not a generally accepted industry method, principle, or guideline for valuing digital assets.

In addition, digital assets are not a homogeneous asset class; they may feature characteristics of securities, commodities, currency units, or a combination thereof. As a result, the valuation analysis applicable to a particular digital asset may involve multiple methods.

Generally, digital assets that have sufficient liquidity and are tradeable on major regulated exchanges may be valued on the basis of the average of the closing day’s spot rate for a given digital asset, as reported by major exchanges and/or industry data sources.

Where no secondary trade pricing exists or liquidity is too low, the valuation of digital assets may be uncertain and influenced by additional factors, such as adoption, market perception, scarcity, expectations of future demand, supply and utility, the results of operations of the issuer, and other macro-economic factors.

While lawyers should understand the foundational concepts of valuation in this space, market participants understand that investment bankers typically perform this work. Even though most investment bankers tend to focus on later-stage companies, where the deal size is generally larger to justify their fees, there are a host of experienced financial professionals who can assist with the valuation process and the negotiation of many other financial terms, which can increase the chances of a successful deal.

Due diligence

Blockchain targets often present a host of complex legal issues. Accordingly, legal due diligence has taken on increased importance in this space.

In addition, blockchain companies often operate in markets that span national borders. Therefore, due diligence investigations should take into account the target's potential plurality of legal regimes, local norms, and practices applicable to it.

While this chapter is not meant to address all of the legal due diligence issues that may arise in a blockchain M&A transaction, the following are key issues worth considering in this space.⁵

U.S. federal securities laws considerations

With over \$31 billion raised via sales of digital assets since 2013, and over 6,678 digital assets in circulation with a combined market capitalisation of approximately \$360 billion,⁶ it should not be surprising that offerings of digital assets (also known as “token offerings”, “initial token offerings”, “token launches”, “token sales”, “initial coin offerings”, or “ICOs”) have become a popular fundraising tool for blockchain companies.

Many blockchain startups launched these offerings from both U.S. and non-U.S. jurisdictions, with some taking the ill-advised position that, for as long as the digital assets being offered were not securities under the laws of the jurisdiction of issuance, there was no need to consider whether such assets constituted securities in the jurisdiction(s) in which they were purchased or may have been purchased.

However, in 2017, the U.S. Securities and Exchange Commission (SEC) clarified that U.S. securities laws do apply when digital assets that qualify as securities are marketed or sold to U.S. persons, regardless of the issuer's location.⁷

As a result, in order for most, if not all, blockchain companies to offer digital assets to U.S. investors in capital-raising transactions, issuers should have, and still should, either: (i) register(ed) the sale of their tokens under Section 5 of the Securities Act of 1933 (the Securities Act) by filing a registration statement, such as on Form S-1 or F-1, with the SEC; or (ii) rely(ied) on an exemption from the registration requirements of the Securities Act, such as Regulation CF, Regulation A and Regulation D. When a target relies on such an exemption, review of the documentation of the target's efforts to comply with the exemption can prove useful in the event of later SEC scrutiny.

In addition, some market participants may have not immediately realised that only digital assets that are not treated as securities – such as bitcoin and ether – can trade freely on cryptocurrency exchanges; however, to the extent it is treated as a security, and is not registered under the Securities Act, a digital asset would be treated as a restricted security, and therefore any sale of such digital asset (*i.e.*, any “secondary sale”) must also be in compliance with similar securities laws and regulations and be transferred from the holder to another person pursuant to an exception or exemption.

Although this basic requirement for secondary sales is similar to the requirement applicable to the initial issuer – *i.e.*, the sale must either be registered or made pursuant to an exemption – the exemptions available for secondary sales and primary sales differ.

In the context of offerings of stock and other traditional securities, these rules tend to be well understood and have been systematised, but they have not been always adequately implemented and respected by many market participants.

Issuers of digital assets who have either engaged in what could be deemed to be an unregistered offering, including by virtue of failing to qualify for an exemption from registration, can consider self-reporting to the SEC, cooperating with the SEC staff during any inquiry or investigation, and the voluntary adoption of remedial measures. Outside the digital asset space, the SEC has settled matters in which cooperation substantially mitigated the sanctions, including that civil penalties were not imposed.⁸

If a blockchain target failed to comply with securities rules and regulations that apply to initial and secondary sales of digital assets, the target may be subject to private securities class actions seeking rescission and damages as well as enforcement actions by U.S. federal and state and/or non-U.S. securities regulators, which may result, and in some cases have resulted, in fines, injunctions, and jail time in connection with potential related criminal proceedings.

Commodities regulation considerations

Digital assets are not a homogeneous asset class; they may feature characteristics of securities, but also commodities, currency units, or a combination thereof. As a result, the legal analysis relating to a particular digital asset should not be limited to whether securities laws are applicable, but instead include multiple regulatory regimes.

Indeed, a potential acquirer should be mindful that cryptocurrencies, whether or not determined to be securities, are treated as commodities (akin to precious metals or physical assets) by the U.S. Commodity Futures Trading Commission (CFTC), which takes the position that all varieties of cryptocurrencies are commodities for purposes of the Commodity Exchange Act.⁹

Since cryptocurrencies are deemed to be commodities, the CFTC has jurisdiction over margined or leveraged transactions in cryptocurrencies that involve “retail” investors (called non-eligible contract participants). Perhaps more importantly, however, by virtue of being deemed a commodity, cryptocurrency transactions imbue the CFTC with anti-fraud and anti-manipulation authority.

As a result, even when securities law anti-fraud and anti-manipulation authority does not reach a particular transaction, commodities law authority does, and a potential acquirer should make sure to conduct a thorough analysis to avoid inheriting potential liabilities or having to address potential pitfalls post-closing.

Federal and state money transmission considerations

In general, unless otherwise exempt, a licence is required to engage in the “business of money transmission” – *i.e.*, to receive and transmit money – under the money transmission laws of each U.S. state in which a person has customers. Separately, a person who is engaged in money transmission activity will generally also be deemed a “money services business” (MSB) under the federal Bank Secrecy Act (BSA), and, as a result, is subject to a registration requirement and related anti-money laundering (AML) compliance programme requirements, which are further addressed below.

The Financial Crimes Enforcement Network (FinCEN), which implements the BSA, has affirmed through guidance that certain activities involving virtual currency – including receiving and transmitting the same – are subject to the BSA requirements (even in cases in which the activity may not be subject to money transmission licensing in a particular state

or states). The BSA also operates to reinforce compliance with state money transmission laws by making it a federal felony to engage in money transmission in a state without a required state money transmission licence in that state.¹⁰

FinCEN has issued extensive guidance on virtual currency activities that constitute MSB activities subjecting a person to the BSA. This guidance establishes that FinCEN interprets its regulations to apply to persons that are administrators or exchangers of virtual currency, as “money transmitters”. An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency. An administrator or exchanger that (1) accepts and transmits a convertible virtual currency, or (2) buys or sells convertible virtual currency for any reason, would be a money transmitter under FinCEN’s regulations, unless a limitation to or exemption from the definition applies to the person.¹¹ Accordingly, the applicability of the BSA to a person’s activities involving virtual currency is a fact-specific inquiry that must be addressed on a case-by-case basis.

Acquirers should be mindful of the fact that some states have interpreted their money transmitter licensing regimes as being applicable to certain activities involving virtual currency, and a number of state money transmission statutes and regulations have been amended to address the regulation of virtual currency. Furthermore, even a state that has not established a formal, public position could conclude that virtual currency activity is covered by the money transmission law. While a state-by-state analysis is beyond the scope of this chapter, market participants should analyse the potential applicability to any particular virtual currency activity of state money transmission licensing laws, as well any guidance, interpretations, enforcement actions or other rulings pertaining to state regulatory approaches to virtual currency activity in order to assess whether the current or contemplated activity of the target would constitute regulated money transmission activity, or require licences under such laws.¹²

What constitutes unlicensed state money transmission activity involving bitcoin was at the heart of a recent federal district court ruling in a criminal AML case suggesting that the transmission of virtual currency on behalf of another person requires a state money transmission licence, even if the state’s money transmission law does not expressly address the regulation of virtual currency.¹³

Even though this case arises out of significant allegations of criminal AML activity, the court’s interpretation of relevant laws appears to suggest a default assumption that money transmission licences are required to receive and transmit virtual currency. In addition, the ruling appears to suggest that other activity involving receiving and transmitting money – even if not historically subject to regulation under state money transmitter licensing laws – could be deemed to constitute engaging in unlicensed money transmission activity in the absence of a formal state interpretation to the contrary.

This interpretation has the potential to significantly disrupt current compliance approaches taken by some organisations engaging in virtual currency activity and could make challenging regulatory due diligence even tougher to perform.

Acquirers should be mindful of the fact that, under federal laws, anyone who knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business could be fined or imprisoned for up to five years.

Finally, it is worth noting that, contrary to the approach suggested by some market participants, it is not sufficient to locate a business offshore in order to avoid U.S. federal registration

and related requirements or U.S. state licensing requirements. In particular, with regard to the registration requirement and related AML compliance programme requirements, the FinCEN regulations apply to an MSB “wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States” and “includes but is not limited to maintenance of any agent, agency, branch, or office within the United States”.¹⁴ On July 26, 2017, FinCEN, working in coordination with the U.S. Attorney’s Office for the Northern District of California, found that BTC-e, also known as Canton Business Corporation, an Internet-based, Russian-located money transmitter that facilitates the purchase and sale of fiat currency and convertible virtual currency, wilfully violated U.S. AML laws.¹⁵ As a result, FinCEN assessed (1) a \$110,003,314 civil money penalty against BTC-e, and (2) a \$12 million civil monetary penalty against BTC-e’s owner and operator, Alexander Vinnik, a Russian national, who was arrested in Greece on July 25, 2017. It is worth noting that this was the first time FinCEN had conducted an action against a foreign money transmitter that is doing business in the United States. FinCEN asserted jurisdiction over BTC-e because a substantial part of its business was with customers in the United States, and some of the servers that participated in the processing of BTC-e’s transactions were located in the United States.

U.S. anti-money laundering considerations

Under the BSA and its implementing regulations issued by FinCEN, a money transmitter engaging in virtual currency activity (or any other activity) that is deemed to be an MSB is required to: (a) register as an MSB with FinCEN; (b) establish and maintain an effective AML programme that is “reasonably designed to prevent the [MSB] from being used to facilitate money laundering and the financing of terrorist activities”; and (c) comply with certain recordkeeping and reporting requirements – including suspicious activity reports (SARs) and currency transaction reports (CTRs).

Generally, an MSB’s BSA/AML programme must be in writing and commensurate with the company’s specific risk profile, *i.e.*, the programme must be risk-based and cannot be an off-the-shelf solution. At a minimum, an MSB’s BSA/AML programme must have the following four components or pillars:

1. policies, procedures, and internal controls that are reasonably designed to assure ongoing compliance with the BSA, in particular with regard to: (a) verifying customer identification; (b) filing reports; (c) creating and retaining records; and (d) responding to law enforcement requests;
2. designation of a person that is responsible for the MSB’s BSA/AML programme (a BSA Officer);
3. provide adequate BSA/AML-related training to all appropriate personnel; and
4. conduct independent (internal or external) testing.

Although not (yet) required by law (but often requested by their banks), many MSBs also establish and implement policies and procedures specifically addressing the identification and verification of beneficial owners of legal entity customers.

An MSB that violates the registration requirement and BSA/AML programme requirements can face enforcement actions from regulators or law enforcement agencies, which may include severe monetary penalties. In addition, engaging in, or aiding and abetting, money laundering is a criminal offence under the U.S. Money Laundering Control Act (MLCA) that is punishable by a maximum of 20 years in prison and fines up to \$500,000 or twice the amount of the transaction involved, whichever is greater. The MLCA applies to all persons

and businesses in the United States as well as to persons and businesses in other countries if at least one part of a transaction is executed in the United States.

It is therefore of utmost importance for an acquirer of a business with virtual currency activities to conduct a thorough AML due diligence in order to determine: (a) whether the target is an MSB that is required to register with FinCEN and have a BSA/AML programme; and, if yes, (b) whether such programme is effective, adequate, and appropriate. We note that there may be additional state legal requirements with regard to an MSB's BSA/AML compliance programme; for example, the New York State Department of Financial Services' (NYDFS) so-called Part 504 requirements, which provide for minimum standards for transaction monitoring and filtering programmes and an annual compliance certification requirement for money transmitters that are licensed by the NYDFS.

Although the above addresses the U.S. legal requirements, many jurisdictions have similar statutory and regulatory frameworks in place, and the following principles generally apply, and should be considered, for transactions involving foreign virtual money transmitters as well.

As with any due diligence, the scope and thoroughness of an AML due diligence should be risk-based. However, at a minimum, an acquirer should review, assess, and understand:

- the target's risk assessment, in particular the specific risks with regard to customers and clients, products and services, and geographic locations;
- all AML-related policies and procedures, including with regard to "know your customer" (KYC), customer due diligence/enhanced due diligence, transaction monitoring and SAR filings, other reporting and recordkeeping requirements, and others;
- independent testing reports and related management responses;
- training materials; and
- structure of the target's BSA/AML compliance department and the BSA Officer's roles and responsibilities.

Further, an acquirer should be mindful to include strong AML-related representations and warranties in any agreement. For effectiveness and efficiency's sake, an acquirer may want to consider combining the AML and sanctions due diligences and closely coordinating these activities.

Considering the legal and reputational risks for being associated with, or being involved in, (alleged) money laundering and terrorist financing activities, an acquirer should also strongly consider conducting at least a limited AML due diligence for any blockchain M&A transaction, even if the target is not directly involved in virtual currency and/or money transmitter activities.

Sanctions considerations

Sanctions refer to legal restrictions governments impose on transactions with specific persons or entire jurisdictions (*i.e.*, embargos). U.S. sanctions are generally strict liability and carry steep fines (for most violations, the greater of approximately \$300,000 or twice the value of the transaction). This creates significant risk for companies that operate in the blockchain space since digital assets may facilitate anonymous or pseudonymous transactions such that blockchain participants could unwittingly engage in transactions prohibited by sanctions.

A number of U.S. sanctions targets, most notably, Iran, North Korea, Russia and Venezuela, have attempted to use blockchain technology to either circumvent U.S. sanctions or engage in malign activity that U.S. sanctions target.

It is then no surprise that the Office of Foreign Assets Control (OFAC), the U.S. agency primarily responsible for implementing and enforcing U.S. sanctions, has taken an interest

in blockchain-related transactions. In November 2018, OFAC sanctioned two Iranian individuals who helped exchange ransom payments from bitcoin to Iranian rials. As part of this action, and for the first time, OFAC added bitcoin wallet addresses to its List of Specially Designated Nationals and Blocked Persons (the SDN List). OFAC has since taken other blockchain-related actions against sanctions targets in Russia and Venezuela who attempted to use a Venezuelan state-sponsored cryptocurrency to circumvent U.S. sanctions against Venezuela.

To avoid the steep fines that come with sanctions violations (and potential reputational risk), acquirer due diligence on targets that develop or use blockchain technology should include a close review of any sanctions controls the target has in place. At a minimum, these should include a process to collect identifying information on blockchain participants, which could include IP address country and screening that information against the SDN List. The target should have IP blocking in place to automatically prevent blockchain participants from facilitating transactions whose IP addresses identify them as located in sanctioned jurisdictions. Additional controls to look for include permissioned blockchains that condition participation on users providing information about their off-chain identities (which can then be screened against the SDN List), or smart contracts that halt transactions when users add sanctions keywords to transaction data such as “Iran” or “Cuba”.

When targets lack appropriate controls to mitigate sanctions risk, acquirers should add indemnifications to purchase agreements that last at least five years to mitigate the risk of undiscovered sanctions violations cropping up after purchase.

1940 Act considerations

The Investment Company Act of 1940, as amended (the 1940 Act), imposes a strict regulatory regime on investment companies that are required to register under the 1940 Act.

An investment company is defined in Section 3 of the 1940 Act, in relevant part, as an issuer primarily engaged in investing in securities or as an issuer that invests or holds 40% or more of its total assets (excluding cash and U.S. government securities) in “investment securities”.

Since many blockchain companies hold digital assets that likely would be deemed securities, it is critical to conduct an investment company analysis to determine whether the proposed target is subject to regulation under the 1940 Act.

To operate in the United States, an investment company must either register as such with the SEC, or fall within an exception or exemption from registration. A non-U.S. investment company cannot register with the SEC without obtaining exemptive relief, which the SEC infrequently provides.

Nevertheless, a non-U.S. investment company could issue securities tokens pursuant to investment company exceptions for issuers that engage in private offerings in the United States either (1) to fewer than 100 U.S. “accredited investors”, or (2) solely to U.S. investors that are “qualified purchasers”.

It is important to remember that an entity that illegally operates as an investment company in the United States is subject to draconian penalties, including the voidability of all contracts.

IP rights considerations

While blockchain-related M&A transactions are relatively new in the M&A landscape, IP rights considerations are simply variations on standard themes. An acquirer of a blockchain target may, however, find additional potential risks, including those related to a more pronounced reliance on open source software, and a greater likelihood of a target being

subject to patent litigation claims. The following are a sampling of IP rights considerations that should be kept in mind when performing IP due diligence of a blockchain target.

A threshold concern when acquiring any IP right is ownership. An acquirer should consider conducting searches of registered IP to establish ownership, applicable jurisdictions in which registrations have been secured, and the periods during which such registrations will remain in effect.

As blockchain technology often includes open source software, the licence terms of such software may impact an acquirer's assessed value of, and ability to exploit, the technology. An acquirer may wish to assess whether open source software is included in the target's software. A careful review of applicable licence terms may be warranted, since open source licences vary from permitting licensees a broad right to use, modify, and distribute software that is based on open source software, to a more restrictive "copyleft" licence that requires the source code of any software based on open source software to be redistributed at no cost.

Acquirers should also confirm chain of title with respect to IP rights, whether registered or not, by confirming that the target has put in place a practice of having all employees, independent contractors, and consultants enter into robust proprietary information and inventions assignment agreements whereby the employees, independent contractors, and consultants are not only obligated to keep all company proprietary information confidential, but agree that whatever they develop, invent, discover, or create during the course of their employment or engagement is owned by the target. Acquirers should also consider whether the target has followed best practices, such as fairly compensating patent owners for their innovations or entering into such arrangements as a patent pool.

Lastly, blockchain-related patents are on the rise not only due to companies investing in their own blockchain-related solutions, but also due to non-practising entities acquiring blockchain-related patents; as a result, companies developing blockchain technology may face a greater number of patent infringement claims than other targets engaged in more conventional businesses. Accordingly, extensive patent due diligence and freedom-to-operate analyses may be advisable.

Privacy and cybersecurity considerations

Unlike IP considerations, using a blockchain in a business model presents novel privacy issues. This is certainly the case when personal information about natural persons is processed on the blockchain, but it is also the case when personal information is stored off-chain but associated with, or linked to from, the chain and even when the information on the chain is not about consumers, but rather about individual business users who are using the blockchain application for business use. Even a user's public-private encryption key associated with their identity is covered by many data protection laws.

Data protection laws around the globe impose requirements and restrictions on processing personal information about individuals, whether they are acting as retail consumers or representatives of businesses. For example, under some laws, called data export restrictions, personal information may only be exported from one country to another if certain conditions are met. This is a challenge for a global blockchain application in which the data is housed and duplicated all over the world. If the blockchain application is private, the data export requirement can be met by including certain terms in the contract between the participants. Similar laws, called data location laws, require that the "master" copy of data be housed in a particular country, even if it may also be stored elsewhere. This poses another challenge for a blockchain application where there is no one true "master" copy.

Data protection laws often also give individuals various rights with regard to companies' use of their data. Sometimes, laws require that individual consent be obtained in order for their data to be used. In a blockchain model, this would require the individual to agree, electronically, to a data agreement before their personal information can be processed on the chain. In some cases, there is no opportunity to obtain this consent directly from the individual, so the participants in the blockchain have to rely on a contractual representation from other participants that they obtained the required consents.

These laws also give individuals the right to request that businesses delete or correct their personal information. Due to the immutable nature of blockchain data, deleting and making changes to data that is stored on the chain is impossible or practically impossible. Therefore, business models that use blockchain must find other ways to honour these requests, such as, possibly, by all participants disposing of a decryption key or by adding a corrective annotation to the data that the individual requested to correct.

Many of these challenges can be avoided by storing personal information off-chain instead of on-chain, and some can be managed by using a private blockchain instead of a public blockchain, so that all participants can agree contractually to the rules of the road for the use of personal information in the blockchain businesses.

CFIUS considerations

An increasingly powerful force that non-U.S. acquirers and U.S. targets (including U.S. subsidiaries and branches of non-U.S. companies) ignore at their peril is the U.S. Committee on Foreign Investment in the United States (CFIUS).

CFIUS is an interagency committee of the U.S. government that reviews certain transactions involving a U.S. business by a non-U.S. person to determine, and potentially mitigate, the effect of such transactions on the national security of the United States, including by addressing any risks associated with the transfer of technology, sensitive personal data, and other resources outside of the United States.

Under the recent regulations implementing the Foreign Investment Risk Review Modernization Act of 2018, CFIUS has the authority to review not only transactions through which a non-U.S. person could gain "control" of a U.S. business, but also certain non-controlling investments in U.S. businesses involving critical technologies, critical infrastructure, or sensitive personal data (so-called TID businesses).

The definition of "critical technologies" includes, among other things, the currently undefined category of "emerging technologies", which likely will comprise certain blockchain technology, among others (other examples include artificial intelligence, quantum computing, robotics, and data analytics).

In addition, a U.S. blockchain target that performs critical infrastructure functions, including by providing Internet protocol networks and exchange points, data centres, and core processing services for financial institutions, telecom, energy, or utility companies, may also fall within CFIUS's heightened scrutiny on non-controlling investments.

Finally, CFIUS may also review certain transactions involving a U.S. blockchain target to the extent it maintains or collects sensitive personal data of U.S. citizens, including financial, geolocation, and health data.

Under relevant statutes and regulations,¹⁶ the president of the United States is authorised to block or unwind acquisitions of, or investments in, U.S. companies by non-U.S. persons when, in the president's view, such transactions threaten the national security of the United States and the threat cannot otherwise be mitigated. In addition, contrary to CFIUS's long-

standing history as a purely voluntary process, certain transactions by non-U.S. persons involving a U.S. TID business are now subject to a mandatory review by CFIUS.

Failure to notify CFIUS of a transaction subject to mandatory filing can result in civil penalties up to the value of the transaction.

In recent years, CFIUS has focused on a substantial number of deals involving non-U.S. acquirers, including British, Canadian, Chinese, and Japanese acquirers. This activity included forcing post-consummation divestitures of Grindr and PatientsLikeMe by two Chinese companies, due to concerns regarding alleged vulnerabilities in cybersecurity and access to sensitive personal data, blocking the takeover of Qualcomm by a Singapore company (before the deal was actually signed), allegedly due to concerns regarding the Singapore company's potential ability to limit Qualcomm's participation and continued advancement of the 5G market, and causing parties to abandon the acquisition of another large U.S. company by a Chinese acquirer, allegedly due to concerns over money laundering and potential threats to the U.S. financial system.

As a result, it is more critical than ever for deal-makers to closely assess the CFIUS risk profile of a blockchain target, and consider whether they must notify CFIUS or, if not, whether they should voluntarily notify CFIUS to seek pre-closing "clearance", *i.e.*, formal confirmation that there are no unresolved national security concerns.

CFIUS-related risk is generally addressed by requiring representations, covenants and a closing condition tied to a successful outcome of the CFIUS review process, and sometimes by including a reverse break fee in the event that the outcome of the CFIUS review process prevents completion of the transaction. Moreover, where the CFIUS risk is high, U.S. targets may consider requesting that the non-U.S. acquirer deposit the amount of the reverse break fee into a U.S. escrow account in U.S. dollars. Non-U.S. acquirers may also consider purchasing CFIUS-risk insurance to cover payment of the reverse break fee, plus other broken deal costs, such as attorneys' fees, investment banking fees, financing costs, and other due diligence expenses, at a cost of approximately 10% to 15% of the reverse break fee.

Tax considerations

Tax due diligence is an important aspect of every M&A deal. All M&A deals should include an analysis of the tax implications at the U.S. federal, U.S. state, local, and international levels. M&A deals involving targets with digital assets require the same due diligence considerations as deals involving targets with more traditional assets. However, M&A deals involving targets with digital assets may have another level of complexity and require additional scrutiny due to the fast-moving pace of the industry. As new and innovative digital assets continue to emerge, taxing authorities have struggled to keep up, which has resulted in a lack of uniformity in reporting and recordkeeping.

For example, for U.S. tax purposes, the Internal Revenue Service has taken the general position that digital assets are treated as property (and, specifically, not as currency, regardless of how the assets may be treated by other governmental authorities). Therefore, tax due diligence applicable to property may broadly be applied and should include an analysis to confirm that the target has been properly reporting and sourcing receipts arising from the digital assets in all jurisdictions (U.S. and international) that may assert taxing nexus.

However, there are often gaps in recordkeeping of digital assets that may result in difficulties about determining even threshold considerations, such as the property's basis. Digital assets are also notoriously difficult to value. Further, it is often difficult to classify the receipts

generated from the holding and selling of digital assets. Typically, attempts to classify such receipts require an analogy to more traditional intangible property. But digital assets do not always have straightforward analogous traditional counterparts. Digital assets may have characteristics of several categories of traditional intangible property, or may have no analogous counterpart at all.

Depending on how a particular digital asset is classified, consideration should also be given to potential depreciation and if the target has been properly depreciating the asset and in the appropriate jurisdiction. For example, under the 2017 Tax Cuts and Jobs Act, tech companies have generally not been able to obtain the benefits of the 100% expensing in connection with asset acquisitions, given that qualifying assets generally include only tangible asset classes and do not include intangible assets. Also, if one or more of the target's digital assets may be considered a capital asset, attention should be given to the holding period of that asset(s), which, along with other considerations, may inform if the transaction should be structured as an asset purchase (which generally would start new holding periods) or a stock purchase (which generally would preserve the holding periods). Finally, depending on the structure of the transaction and the classification of the digital assets, acquirers should be aware of potential transfer tax liabilities that may arise as a result of the deal.

Blockchain integration

Unique hurdles relate not only to valuation and due diligence but also to the post-closing integration phase, which is often the most critical measure of long-term M&A success, so critical that acquirers often consider the first quarter(s) after closing a predictor of the likelihood of success of the overall transaction.

Serial acquirers often have a well-established integration process; however, no two integration programmes are exactly alike, and the integration of fast-growing blockchain companies often requires reshaping traditional strategies that allow the target to maintain some autonomy but also actively participate in the integration process.

Integration planning should be carefully analysed ahead of time since its implementation may require time-consuming tasks, including addressing multiple cultures, languages, business practices, and processes, social and political landscapes, legal frameworks, and approvals of local regulatory authorities.

In practice, we note that parties to a blockchain-related M&A transaction often meticulously focus on three main integration-related hurdles: the technology stack; culture; and legal compliance.

Hurdles to technological integration

Typically, technology integration is the most challenging and costly element of any blockchain M&A deal.

As a relatively novel technology, blockchain has not undergone the standardisation procedures that might lead to widespread adoption of one or two universal technical standards. Currently, several developers are competing for their blockchain standard to come out on top; in the meantime, virtually none of the blockchains or services built on top of them are able to communicate with one another. Decentralised and public blockchains are particularly vulnerable, and developers often have to expend valuable resources to make their services accessible across different blockchains.

For companies considering a blockchain enterprise solution, these different technologies' inability to communicate with one another or with more centralised legacy software could significantly diminish a transaction's long-term value and overall success. Until the blockchain industry (and its many consortia) settle on a single technical standard or interoperability solution, careful consideration of how a newly acquired blockchain technology will integrate into an existing technology stack may remain a significant hurdle, particularly for new entrants into the blockchain market.

Therefore, both acquirers and targets should consider including their respective IT experts in the due diligence process and make sure they analyse the costs and practical realities related to effectively retrofitting a blockchain-enabled technology into the acquirer's IT infrastructure. At least at some level, while developers work with operations and finance experts to develop a long-term, comprehensive integration plan, maintaining separate operating systems might be the preferable choice.

In addition, in anticipation of a blockchain acquisition, acquirers should consider developing a flexible IT infrastructure that allows, among other things, the effortless migration of new data gained from the target. However, there may still be incompatibilities between the existing IT systems or back-office support systems that adversely impact data migration. Adopting temporary workarounds, including operating duplicate systems during a transitional period, may make good business sense, at least in the beginning. Finally, existing servers may not have the capacity to handle the combined businesses, and upgrades or additional investment in relevant equipment may be required.

Hurdles to cultural integration

Navigating the issues surrounding compensation and benefits is always a sensitive consideration in any M&A deal. However, while parties tend to see value in capitalising on each other's strengths, what they often overlook, to their detriment, is to what extent there is cultural compatibility or lack thereof, which is especially critical when they operate in different industries (*i.e.*, tech and non-tech). What at first glance may often appear to be cultural alignment in mission can quickly devolve into profound operational and ideological clashes that can affect the abilities of the different stakeholders to efficiently collaborate post-closing and the overall success of the integration strategy.

As an example, acquirers not familiar with the unique history of blockchain should be aware that many blockchain startups, particularly those working closer to decentralised public blockchains, feature an agile culture where employees are encouraged to put forward new ideas and are generally accustomed to rapid change, ambiguities, and risk in order to drive innovation. Most blockchain teams do not necessarily view the top-down decision-making, structural controls, discipline, well-defined processes, or the reassuring predictability of legacy companies as ideal or consistent with their ethos. Moreover, it is no secret that skilled employees are in demand; most of them are often millennials who are passionate about creating technology with social impact and expect to continue learning "on the job" in a collaborative environment while retaining autonomy and access to the latest tools and technologies. Eliminating seemingly unnecessary perks, such as a token incentive plan, ample bandwidth to choose non-traditional titles, or even unlimited kombucha on tap, or adding an additional layer of bureaucracy could negatively impact the employees' morale and overall productivity, disrupt the creative spirit that made the target succeed, and, in the worst but not uncommon scenario, push talented people to look for greener pastures.

While the intention of making changes is often meant to create uniformity and reconcile cultural differences, the integration team should consider leaving certain customs intact or

staggering the timing of any changes while providing clear communication, *i.e.*, explaining why some changes are necessary and ought to be implemented (as opposed to just saying “this is the way we do things around here”) and allowing employees to voice any concerns or suggestions.

Most importantly, both acquirers and targets should conduct a cultural assessment as part of their due diligence ahead of time; it is crucial to identify any potential threats posed by differing cultures. Parties should also be prepared to negotiate certain aspects of their culture by identifying areas where a bit more structure would likely not hurt, and somewhat looser features may likely be welcome, and then continually reevaluate their original integration strategy.

Hurdles to legal compliance

While many critical issues regarding the integration of blockchain technology are often left to IT, HR, and business specialists, outside legal counsel should add value with respect to a few critical issues and otherwise oversee the integration process alongside in-house counsel.

Successful integration begins with legal due diligence. While outside counsel is often asked to focus on certain substantive areas that may affect valuation or the negotiation of the representations and warranties set forth in the purchase or merger agreement, counsel should also evaluate the integration plan from a legal compliance perspective in order to address any needs for remediation post-closing. Particularly in cross-border transactions, parties to a blockchain M&A deal should involve appropriate specialists as early in the process as possible to ensure compliance with all applicable laws and regulations.

For example, according to the Federal Trade Commission, “one company’s purchase of another doesn’t nullify the privacy promises made when the data was first collected”.¹⁷ As a result, in the event a blockchain target’s privacy and data security policies exceed or are otherwise more robust than the acquirer’s, then the acquirer may need to: (i) comply with the target’s applicable policies and continue to handle data as promised when the target collected it; or (ii) segregate the data.

In addition, data migration plans may be affected by a myriad of applicable laws, particularly in cross-border deals; therefore, counsel should analyse any privacy restrictions that may limit the sharing or transfer of data and work with local counsel.

Acquirers should also keep in mind that software licences may include provisions that limit the number of users, which could be breached due to the transaction or by increased users after the transaction.

Finally, depending on the nature of the blockchain target, and whether any aspects of its business are regulated, the acquirer and the target may be required to obtain, renew, or modify permits or licences in various jurisdictions. Therefore, details of any activities that may be limited or restricted pending receipt of such regulatory permits or licences should also be included in the integration plan and closely monitored.

Reaping the rewards

2020 has been the year of normalisation for blockchain technology: the valuations have generally stabilised; the deal flow has remained virtually steady; and the enterprise use cases have become more apposite than ever.

For deal-makers seeking to create synergies, drive growth, or enter new markets in uncertain times, blockchain M&A may be the answer; with expert deal analysis and proper planning, any strategic and financial acquirer has the opportunity to employ M&A and become the next link in the evolution of blockchain.

Endnotes

1. In this chapter, we generally refer to “M&A” to include partnerships, joint ventures, mergers and acquisitions, and other strategic and private equity transactions.
2. See Research.Tokendata.io.
3. In this chapter, we generally refer to “digital assets” to include cryptocurrencies, security tokens, decentralised application tokens, protocol tokens, and other similar blockchain-enabled instruments, the ownership and/or transmission of which is recorded or verified by a distributed ledger (including a “blockchain” or directed acyclic graph) or other similar technology. We note, however, that market participants generally refer to: (i) “cryptocurrencies” to mean a digital representation of value that functions as a medium of exchange, a unit of account, or a store of value, which is generally used as a substitute for fiat currencies as a means of paying for goods or services or transferring value, and is not meant to be a “security”, as such term is defined under U.S. federal securities laws (bitcoin and ether are examples of such cryptocurrencies); and (ii) “security tokens” to mean broadly blockchain-enabled assets that fall within the definition of a security under U.S. federal securities laws.
4. See *The Most In-demand Jobs: Where the Opportunity Is Now*, available at <https://blog.linkedin.com/2020/may/june/18/the-most-in-demand-jobs-where-the-opportunity-is-now>.
5. Here, we focus on diligence of legal issues more prominent among blockchain companies generally; however, acquirers will also need to consider more company-specific issues, including issues relating to specific assets and actual or potential liabilities, including stockholder issues and employment and contractor-related liabilities, employee benefits, and the blockchain company’s contracts.
6. See ConMarketCap.com.
7. See, e.g., *In the Matter of SAP SE*, Adm. Proc. File No. 3-17080 (February 1, 2016).
8. In addition, in April 2019, the SEC’s Strategic Hub for Innovation and Financial Technology (FinHub) published additional informal guidance, titled “Framework for ‘Investment Contract’ Analysis of Digital Assets”, which provides analytical tools for determining whether a digital asset is a security based on an analysis of whether the asset is an “investment contract”, as that term was first used by the Supreme Court of the United States in *SEC v. Howey*, 328 U.S. 293 (1946).
9. The term “commodity”, defined in Section 1a(9) of the Commodity Exchange Act, is extremely broad, covering everything from physical commodities to “services, rights, and interests”, which the CFTC believes includes cryptocurrencies, and are therefore subject to the CFTC’s jurisdiction.
10. See 18 U.S.C. § 1960(b)(1)(B).
11. See FIN-2013-G001, *Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (March 18, 2013).
12. State money transmission licensing laws generally define regulated activity broadly to include “receiving money for transmission” and many state statutes define “money” to include “monetary value”. Any state that has to date not established a formal position with respect to the regulation of virtual currency activity could: (1) deem the receipt, holding, or transfer of fiat currency in connection with virtual currency activity (such as facilitating a virtual currency exchange platform) to constitute money transmission subject to regulation in its own right; and (2) deem virtual currency activity itself to be subject to regulation in a manner similar to activity involving fiat currency, such as receiving and transmitting virtual currency.

13. See *U.S. v. Harmon*, Case 1:19-cr-00395-BAH (D.D.C. Jul. 24, 2020).
14. See 31 CFR § 1010.100(ff)(5).
15. See *In the Matter of BTC-E*, No. 2017-3, at 2 (Jul. 27, 2017), available at https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf.
16. See 31 CFR Part 800.
17. See *Mergers and privacy promises*, available at <https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises>.

* * *

The views expressed in this chapter are solely of the author and do not necessarily represent the policies or views of Morrison & Foerster LLP or any of its partners.

* * *

Acknowledgments

The author would like to thank the invaluable contributions of Susan Gault-Brown, Michael G. O'Bryan, Charles L. Capito, Marc-Alain Galeazzi, Vivian L. Hanson, Kristen J. Mathews, Sean Ruff, John E. Smith, Rebecca M. Balinskas, Panagiotis (Aki) C. Bayz, Edward L. Froelich, Adam J. Fleisher, Joan Kim, Lee Adam Nisson and Kristofer G. Readling. It takes a village!

**F. Dario de Martino****Tel: +1 212 336 4156 / Email: DdeMartino@mofocom**

Dario de Martino is a partner in the New York office of Morrison & Foerster LLP and is a member of the firm's Mergers + Acquisitions Group.

He has a wide range of experience representing U.S.-based and global technology, financial services, healthcare and industrial companies with respect to their domestic and cross-border mergers & acquisitions, carve-outs, joint ventures, and other complex strategic and private equity transactions.

Mr. de Martino serves as the Co-Chair of the firm's Blockchain + Smart Contracts Group and regularly counsels some of the most influential market participants with respect to a variety of matters relating to blockchain, tokenisation, cryptocurrencies, and smart contracts. His experience in the digital asset space includes advising public and private companies with respect to blockchain M&A, strategic and private equity transactions, digital assets offerings, blockchain licensing and service agreements, and new blockchain-enabled products that implicate securities or commodities/derivatives laws.

He is a frequent speaker and writer on various topics in M&A and private equity with a particular focus on innovative technologies.

He is also an active leader in the firm's diversity, equity and inclusion initiatives.

Morrison & Foerster LLP250 West 55th Street, New York, NY 10019-9601, USATel: +1 212 468 8000 / URL: www.mofocom

Untying the Gordian Knot – Custody of digital assets

Richard B. Levin, David M. Allred & Peter F. Waltz
Polsinelli PC

Like the Gordian Knot solved by Alexander the Great, regulators in the United States have attempted to craft a clean solution to the complex problem of the custody of digital assets.¹ Starting with the Great Depression, regulators in the United States have focused on the safety and soundness of locations holding customer funds or securities. As investors have become increasingly interested in digital assets, U.S. regulators have faced the challenge of attempting to protect customer funds and securities using laws written in the 1930s, 1940s, and 1970s. Unfortunately, these laws were not designed to regulate custody of digital assets. In this chapter, we provide an overview of digital assets and the technology used to hold digital assets, including Bitcoin, followed by a focus on the current state of the regulation of custody of digital assets by the U.S. Securities and Exchange Commission (“SEC”), the U.S. Office of the Comptroller of the Currency (“OCC”), and the New York Department of Financial Services (“NYDFS”).

Background

Blockchain technology is a database structure that can only be updated by appending a new set (or block) of valid transactions to the log of previous transactions.² As noted by Goldman Sachs in a note to clients:

In its most basic form, the blockchain records ownership of bitcoin and transactions involving the crypto currency across a wide network of computers, as opposed to a centralized ledger. Transactions are signed off by the parties involved using the software, checked by the network or the “crowd,” then added to the blockchain – a long string of code that records all activity. Encryption in the software ensures these “blocks” cannot be tampered with or altered. And the decentralized nature means the “crowd” police the whole system. The software cuts out the need for a “trusted middleman” to sit in between parties in a transaction, such as a bank or clearinghouse. This makes transactions quicker, cheaper, and easier when compared to the current systems banks use.³

Many firms in the financial services industry believe blockchain technology can be adapted for use in traditional financial services transactions in a way that *“has the potential to redefine transactions and the back office of a multitude of different industries.* From banking and payments to ... trade settlement ... a distributed shared ledger has the potential to make interactions quicker, less-expensive and safer”.⁴

Digital currencies

Digital currencies are monetary units of exchange stored or represented in a digital or other electronic format that operate like currency in some environments, but that do not have

legal tender status in any jurisdiction.⁵ The term digital currency refers to electronic money that operates like a currency in some environments, but does not have all the attributes of “real” (i.e., fiat) currency issued by a governmental agency.⁶ Digital currencies can be created by an individual, corporation, or organisation, or can arise from use and acceptance by people as currency.⁷ Traditional currencies are generally either backed by the faith and credit of the national governments that recognise the currency (the fiat system) or by real assets or hard commodities, such as gold, silver, or minerals (the commodity system).

Blockchain and the SEC

The focus of the financial services industry on blockchain technologies has attracted the attention of the SEC, which has published several pieces of guidance on blockchain technology and has hosted events such as a FinTech Forum that included a panel discussion on blockchain technologies.⁸ The SEC has noted:

[T]he blockchain ... is being tested in a variety of settings, to determine whether it has utility in the securities industry. What utility, if any, would a distributed public ledger system have for transfer agents, and how would it be used. What regulatory actions, if any, would facilitate that utility? *How would transfer agents ensure their use of or interaction with such a system would comply and be consistent with federal securities laws and regulations, including the transfer agent rule?*⁹

Advocates of blockchain technology believe it could substantially improve the trading, clearance and settlement of securities.¹⁰ SEC Commissioner Kara Stein noted “one could imagine a world in which securities lending, repo, and margin financing are all traceable through blockchain’s transparent and open approach to tracking transactions”.¹¹

Digital assets

The SEC has defined digital assets as “an asset that is issued and transferred using distributed ledger or blockchain technology”.¹² Digital assets include, but are not limited to, virtual currencies, coins, and tokens.¹³ A digital asset may in certain instances be deemed a security under the federal securities laws. While not defined in the securities laws, the SEC often refers to digital assets that are securities as “digital asset securities”.¹⁴

Wallets and keys

Digital assets are stored by associating them with addresses called “wallets” which can be stored on web servers, local hardware like personal computers, jump drives and mobile devices, or on paper print-outs.¹⁵ A digital asset wallet takes the form of a cryptographic public key, which is a string of numbers and letters.¹⁶ Each public key has a matching “private key”, known only to the user.¹⁷ Control of the private keys is what assures one of control of the digital assets at any address, so collections of private keys must be protected by passwords or other means of securing them.¹⁸ The question of the custody of digital assets that are securities presents substantial problems for firms registered with the SEC as an investment adviser or a broker-dealer.

Digital asset securities

The definitions of “security” under the Securities Act of 1933 (the “Securities Act”) and the Securities Exchange Act of 1934 (the “Exchange Act”) are virtually identical and each is broad enough to include the various types of instruments that are used in commercial marketplaces that one might suspect to fall within the ordinary concepts of a security.¹⁹ This includes common instruments like stocks, bonds, and notes, as well as the various collective investment pools and common enterprises devised by persons seeking to generate profits from the efforts and investments of others (i.e., investment contracts

and instruments commonly known as securities).²⁰ The definitions of security under the Securities Act, the Exchange Act, the Investment Advisers Act of 1940 (the “Advisers Act”), and the Investment Company Act of 1940, do not include currencies. However, the SEC has argued that investments in digital asset-related schemes are investment contracts – a contract, transaction, or scheme involving (i) an investment of money, (ii) in a common enterprise, (iii) with the expectation that profits will be derived from the efforts of the promoter or a third party.²¹

Assuming you agree with the Chairman of the SEC that nearly all digital assets that have been issued to date are securities,²² the custody of such securities by investment advisers and broker-dealers registered with the SEC will require the application of existing securities laws that address custody and protection of customer funds and securities.

Investment advisers

The Advisers Act defines an “investment adviser” as any person who, for compensation, engages in the business of providing advice to others or issuing reports or analyses regarding securities.²³ A person must satisfy all three elements to fall within the definition of “investment adviser”.

The Custody Rule

A registered adviser with custody of client funds or securities (“client assets”) is required by Rule 206(4)-2 of the Advisers Act (the “Custody Rule”) to establish a set of controls to safeguard those assets.²⁴ Custody means “holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them”.²⁵ An adviser is deemed to have custody if an affiliate has custody of its client funds or securities in connection with advisory services it provides to clients. Custody includes:

- *physical possession of client funds or securities;*
- any arrangement under which an adviser is permitted or authorised to withdraw client funds or securities (such as check-writing authority or the ability to deduct fees from client assets); and
- *any capacity that gives an adviser or its supervised person legal ownership of or access to client funds or securities.*²⁶

An investment adviser is deemed to have custody if it or a related person holds, directly or indirectly, client funds or securities, or has any authority to obtain possession of them.²⁷

Qualified custodians

An adviser with custody must maintain client funds and securities with a qualified custodian either under the client’s name or under the adviser’s name as agent or trustee for its client.²⁸ A qualified custodian is a federally insured bank or savings association, a registered broker-dealer, a registered futures commission merchant (with respect to client funds and security futures), or a foreign financial institution that customarily holds financial assets for its customers.²⁹ A “bank” is defined as:

- a *banking institution* organised under the laws of the United States or a federal savings association;
- a member bank of the Federal Reserve System; or
- any other banking institution, savings association, or *trust company, whether incorporated or not, doing business under the laws of any state or of the United States*, a substantial portion of the business of which consists of receiving deposits or exercising fiduciary powers similar to those permitted to national banks under the authority of the Comptroller of the Currency, and which is supervised and examined by state or federal authority having supervision over banks or savings associations.³⁰

The qualified custodian must send an account statement at least quarterly to each client, and client funds and securities must be verified at least annually by an independent public accountant.³¹

Client assets that are not cash or securities need not be maintained with a qualified custodian. Two types of securities are not required to be maintained with a qualified custodian: (i) shares of mutual funds held with the fund’s transfer agent; and (ii) privately offered securities (i.e., uncertificated securities acquired in a private placement that are recorded in the name of the client only on the books of the issuer or its transfer agent and transferrable only with the consent of the issuer).³²

Since most digital asset securities are uncertificated securities, and assuming they were sold in a private placement under a safe harbour from registration under the Securities Act, such as Regulation D, such digital assets should not be subject to the Custody Rule. However, many digital asset securities, including the majority of those issued in the initial coin offering boom of 2016–2018, likely were not sold in compliance with federal securities laws. Any digital assets securities that are registered with the SEC and that are held by a registered investment adviser on behalf of a client are subject to the Custody Rule.

SEC Guidance on custody of digital assets by investment advisers

The SEC has deemed client digital assets that are not securities to be client funds. On March 12, 2019, the staff of the SEC Division of Investment Management (the “Division”) published a letter seeking input from investment advisers, other market participants, and the public regarding the application of the Custody Rule to digital assets.³³ That letter was a response to issues raised by investment advisers and other market participants following the publication of SEC Guidance on the issue in 2017.³⁴ In the letter, the SEC staff noted digital assets are subject to the Custody Rule if they are either “funds” or “securities” and if the registered investment adviser has any authority to obtain possession of them.

On January 18, 2018, the Director of the Division sent a letter to the Investment Company Institute and the Securities Industry Financial Markets Association, captioned “Engaging on Fund Innovation and Cryptocurrency-related Holdings”.³⁵ In the letter, the SEC staff noted:

*We appreciate that proponents of cryptocurrencies and related products have identified a range of potential benefits. ... [T]he innovative nature of cryptocurrencies and related products, as well as their expected use and utility in our financial markets, means that they are, in many ways, unlike the types of investments that registered funds currently hold in substantial amounts.*³⁶

In the letter, the Division requested information on several investor protection issues before sponsors begin offering these funds to retail investors, including the custody of digital assets that are securities.³⁷ The Division noted the Advisers Act requires the use of safeguards to ensure that registered funds maintain safe custody of their holdings custodian.

Broker-dealers

Like registered investment advisers, broker-dealers must comply with rules that are designed to protect customer funds and securities, including Rule 15c3-3 of the Exchange Act (the “Customer Protection Rule”). The Customer Protection Rule is meant to prevent investor loss or harm in the event of a broker-dealer’s failure and to enhance the SEC’s ability to monitor and prevent unsound business practices. The rule requires a broker-dealer to physically hold customers’ fully paid and excess margin securities or maintain them

free of lien at a *good control location*.³⁸ Generally, a broker-dealer may custody customer securities with a third-party custodian (e.g., the Depository Trust Company or a clearing bank),³⁹ and uncertificated securities may be held at the issuer or at the issuer’s transfer agent.⁴⁰ The question of how a broker-dealer may custody digital assets that are securities has plagued FinTech firms and broker-dealers since 2009.

In July 2019, the SEC staff and the staff of the Financial Industry Regulatory Authority (“FINRA”) published a statement to broker-dealers that plan to facilitate transactions in digital assets that are securities, including the custody of such securities.⁴¹ The SEC and FINRA staff addressed how broker-dealers can comply with aspects of the Customer Protection Rule.

Non-custodial broker-dealer models for digital asset securities

The Joint Statement notes that some entities have contemplated engaging in broker-dealer activities involving digital asset securities that would not involve the broker-dealer engaging in custody functions. The SEC and FINRA staff identified the following examples of business activities presented by FinTech companies:

- A broker-dealer sends the trade-matching details to the buyer and issuer of a digital asset security (similar to a traditional private placement), and the issuer settles the transaction bilaterally with the buyer away from the broker-dealer. The broker-dealer instructs the customer to pay the issuer directly and instructs the issuer to issue the digital asset security to the customer’s digital wallet.
- A broker-dealer facilitates a secondary market transaction in digital asset securities and does not take custody or control over the digital asset securities. The buyer and seller complete the transaction directly. The digital asset securities do not pass through the broker-dealer facilitating the transaction.
- A secondary market transaction involves a broker-dealer introducing a buyer to a seller of digital asset securities through a broker-dealer that operates an alternative trading system (“ATS”).⁴² The ATS brings together the buyer and the seller of digital asset securities. The trades are settled directly between the buyer and seller, or the buyer and seller would give instructions to their respective custodians to settle the transactions. The ATS will not guarantee or have responsibility for settlement of the trades and will not at any time exercise any level of control over the digital asset securities being sold or the cash being used to make the purchase. The ATS will not place a temporary hold on the seller’s wallet or on the buyer’s cash to ensure the transaction is completed.

These are only some of the examples presented to the SEC and FINRA staff.⁴³

Custody of digital asset securities

The SEC and FINRA staff acknowledged in the Joint Statement that market participants wishing to custody digital asset securities might find it challenging to comply with the Customer Protection Rule without putting in place significant unique technological solutions. However, the SEC and FINRA staff reiterated their desire to engage with FinTech firms so that they may better respond to developments in the market⁴⁴ while advancing the missions of the respective organisations: for the SEC, to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation; and for FINRA, to provide investor protection and promote market integrity.⁴⁵

The Customer Protection Rule and digital asset securities

In the Joint Statement, the SEC and FINRA staff noted a broker-dealer seeking to custody digital asset securities must comply with the Customer Protection Rule. Rule 15c3-3

requires a broker-dealer to physically hold customers' fully paid and excess margin securities or maintain them free of lien at a *good control location*.⁴⁶ Generally, a broker-dealer may custody customer securities with a third-party custodian (e.g., the Depository Trust Company or a clearing bank),⁴⁷ and uncertificated securities at the issuer or at the issuer's transfer agent. In either case, a third party controls the transfer of the securities.

Suitable control location

The Customer Protection Rules require customer funds and securities be held at a custodian that meets the definition of a "bank" under Section 3(a)(6) of the Exchange Act. Section 3(a)(6) of the Exchange Act defines a bank as:

(A) a banking institution organized under the laws of the United States, (B) a member bank of the Federal Reserve System, (C) *any other banking institution, whether incorporated or not, doing business under the laws of any State or of the United States, a substantial portion of the business of which consists of receiving deposits or exercising fiduciary powers similar to those permitted to national banks under the authority of the Comptroller of the Currency ... and which is supervised and examined by State or Federal authority having supervision over banks ...*

Banks that are regulated by the Federal Reserve meet the definition of a "bank" under Section 3(a)(6) of the Exchange Act.

The SEC has not issued formal guidance on whether a state-chartered trust company is a bank for purposes of Section 3(a)(6) of the Exchange Act or a suitable control location for purposes of the Customer Protection Rule. There is a tenable argument that a state-chartered trust company is a bank for purposes of the Exchange Act because it is doing business under the laws of a state of the United States, so long as a substantial portion of the business of the trust company consists of receiving deposits or exercising fiduciary powers similar to those permitted to national banks under the authority of the Comptroller of the Currency.

OCC regulation of custody of digital assets

On July 22, 2020, the OCC published an interpretive letter recognising that a national bank may provide custody services for cryptocurrencies, including storage of the cryptographic keys that permit the control and transfer of the customer's cryptocurrency.⁴⁸ The letter recognised past OCC interpretive letters that authorise national banks to provide similar services such as escrow encryption keys used in connection with digital certificates, and secure web-based document storage, retrieval and collaboration of documents and files containing personal information or valuable confidential trade or business information.⁴⁹ The letter notes providing custody for cryptocurrencies will require a bank to provide custody for cryptographic keys. The OCC stated prior letters establish that national banks have the authority to provide custody for this type of digital asset.⁵⁰ The OCC also affirmed the agency's belief in its own expansive power to "authorize national banks to perform, provide or deliver through electronic means and facilities any activities that they are otherwise authorized to perform".⁵¹

National banks have declined to provide custody services for cryptocurrencies and other digital assets because of the lack of clarity on the permissibility of custody of digital assets. While some state-chartered trust companies have provided these services, the majority of state banks have also declined to do so because of the lack of regulatory clarity. The OCC guidance may expand the number of banks that are willing to provide custodial services for digital assets, which will enable more institutions and individuals to invest in digital assets.

The OCC letter may also enable registered investment advisers, which are required to maintain custody of their assets at banks under the Investment Company Act⁵² to hold cryptocurrencies. The OCC letter may also enable registered investment advisers with retail customers, whose assets are commonly held in brokerage accounts, to advise on cryptocurrencies. Finally, the OCC letter may enable broker-dealers to hold cryptocurrencies in customer accounts consistent with the requirements of the Customer Protection Rule.⁵³

While there are tenable arguments that banks regulated by the OCC and state-chartered trust companies may hold digital assets for customers, the issue is complicated by the State of New York's regulation of digital assets.

New York regulation of custody of digital assets

On June 24, 2015, NYDFS adopted regulations on virtual currency businesses in New York State.⁵⁴ Under the regulations, any person that is a resident of or located in, or has a place of business or is conducting business in, New York, and is engaged in a “virtual currency business activity”, is required to obtain a licence from NYDFS. Licensed virtual currency businesses must: (i) have in place certain compliance policies; (ii) meet capital requirements set by NYDFS on a case-by-case basis; (iii) *meet prescribed customer protection and asset custody standards*; (iv) keep certain required books and records subject to NYDFS examinations; (v) have implemented anti-money laundering and cyber security programmes; (vi) have a business continuity and disaster recovery programme in place; and (vii) establish and maintain a customer complaints process.⁵⁵

BitLicense

A three-step analysis helps determine if a business must obtain a BitLicense. First, the entity must offer a product or service that involves a “virtual currency”. NYDFS Rule 200.2(p) defines “virtual currency” to include “any type of digital unit that is used as a medium of exchange or a form of digitally stored value”.⁵⁶ If the business involves a virtual currency, the analysis turns to whether the business is engaged in a “virtual currency business activity”. The regulations define the term “virtual currency business activity” as the conduct of one or more of several types of activities involving New York or a New York resident, including, among others:

- *storing, holding, or maintaining custody or control of virtual currency on behalf of others*;
- performing Exchange Services as a customer business;⁵⁷ or
- *controlling, administering, or issuing a virtual currency*.⁵⁸

The development and dissemination of software alone does not constitute a virtual currency business activity.⁵⁹ However, the act of serving as a custodian of virtual currency in New York or for New York residents brings a party within the scope of the BitLicense, unless they fall within the scope of an exemption from registration.

Exemptions

The BitLicense regulations provide limited exemptions from the licensing requirement for entities chartered under the New York Banking Law and “merchants and consumers using virtual currency solely for the purchase of goods or services or for investment purposes”.⁶⁰ A firm that is subject to regulation by a functional federal regulator, including the OCC, the SEC, or a futures commission merchant registered with the U.S. Commodity Futures Trading Commission, would be required to obtain a BitLicense if it performs any of the functions discussed above. In addition, because the exemption is only for entities chartered under the New York Banking Law, money transmitters registered with the U.S. Office of Financial

Crimes Enforcement Network, and licensed by NYDFS or other states, are not exempt from the BitLicense licence requirement.⁶¹ Agency principals also do not apply to licensing requirements for the BitLicense as they otherwise might within other regulatory regimes.

Reciprocity

The BitLicense regime does not provide for any reciprocity for persons similarly registered in other states. Accordingly, a custodian that is not chartered under the New York Banking Law will have to obtain a BitLicense to provide custody of digital assets for New York residents.

Limited purpose trust charter

In New York, virtual currency businesses are exempt from the BitLicense requirements if they are chartered under the New York Banking Law as a limited purpose trust company, and are approved by the superintendent to engage in virtual currency business activity.⁶² An entity chartered as a New York limited purpose trust company must obtain approval from NYDFS when there is a change in the general character of its business or a change in its corporate structure or control.⁶³ Under the limited purpose trust charter, an entity must comply with similar regulatory compliance requirements as required by the BitLicense.

Conclusion

The issue of custody of digital assets is a complex problem that has plagued the development of the FinTech industry. Investment advisers and broker-dealers that have custody or control of digital assets securities must attempt to reconcile the Custody Rule and the Customer Protection Rule that were not designed for securities that are digital assets. However, the SEC and FINRA have attempted to fit the proverbial square peg into the round hole by applying the Customer Protection Rule and the Custody Rule to digital assets securities. In both cases, broker-dealers and investment advisers can use entities that meet the definition of a bank under the Advisers Act and the Exchange Act, including state trust companies. While the recent guidance from the OCC states that national banks may hold digital assets, the letter does not address whether such assets are protected by the Federal Deposit Insurance Corporation. Finally, while trust companies in certain states may be authorised to hold digital assets, the New York BitLicense limits the ability of such firms to provide services in all states because the BitLicense regime does not recognise trust companies that are chartered in other states as being exempt from the registration requirement. While blockchain technology holds tremendous promise for the financial services industry, the regulation of custody of digital assets will continue to slow innovation in the industry until such time as regulators completely untie the knot of how to reconcile 21st century technology with laws written in the early 20th century.

* * *

Endnotes

1. In this chapter, we use the term the term “digital asset” which refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology, including virtual currencies, coins, and tokens. A digital asset may meet the definition of a “security” under the federal securities laws. For the purposes of this chapter, a digital asset that is a security is referred to as a “digital asset security”.
2. PricewaterhouseCoopers, 2016. *What is the blockchain?* Available at: <http://www.pwc.com/us/en/financial-services/publications/qa-what-is-blockchain.html> (last visited Sep. 23, 2020).

3. Goldman Sachs, *Emerging Theme Radar: What if I Told You...* (2015), available at: <https://www.goldmansachs.com/insights/pages/macroeconomic-insights-folder/what-if-i-told-you/report.pdf#:~:text=Emerging%20Theme%20Radar%20What%20if%20I%20Told%20You...to%20creating%20a%20alternative%20to%20fossil%20fuel%20in> (last visited Sep. 23, 2020).
4. *Id.*
5. Financial Crimes Enforcement Network (“FinCEN”) (2013). Guidance FIN-2013-G0001: Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. United States Department of the Treasury, New York, available at: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (last visited Sep. 23, 2020).
6. *Id.*
7. Turpin, J., *Bitcoin: the economic case for a global, virtual currency operating in an unexplored legal framework*. Ind. J. Global Legal Stud. 21 (1), 335–368 (2014), available at: <http://www.repository.law.indiana.edu/ijgls/vol21/iss1/13/> (last visited Sep. 23, 2020).
8. SEC FinTech Forum, available at: <https://www.sec.gov/spotlight/fintech> (last visited Sep. 23, 2020).
9. Securities Exchange Act Release No. 76743 (Dec. 22, 2015), 80 Fed. Reg. 81948 (Dec. 31, 2015) (“Transfer Agent Release”), available at: <https://www.sec.gov/rules/concept/2015/34-76743.pdf> (last visited Sep. 23, 2020).
10. *Id.*
11. Stein, K., 2015. Speech, *Surfing the Wave: Technology, Innovation, and Competition* – Remarks at Harvard Law School’s Fidelity Guest Lecture Series, available at: <https://www.sec.gov/news/speech/stein-2015-remarks-harvard-law-school.html> (last visited Sep. 23, 2020).
12. *Statement on Digital Asset Securities Issuance and Trading*, Division of Corporation Finance, Division of Investment Management, and Division of Trading and Markets, SEC (Nov. 16, 2018), (“Statement of Digital Asset Securities”) available at: <https://www.sec.gov/news/public-statement/digital-asset-securities-issuance-and-trading> (last visited Sep. 23, 2020).
13. *Id.*
14. *Id.*
15. Levin, R., O’Brien, A., and Zuberi, M., *Real Regulation of Virtual Currencies*, Handbook of Digital Currency (2015).
16. *Id.*
17. *Id.*
18. *Id.*
19. Levin, R., Waltz, P., and LaCount, H., *Betting Blockchain Will Change Everything – SEC and CFTC Regulation of Blockchain Technology*, Handbook of Blockchain, Digital Finance, and Inclusion, Volume II (2016).
20. *Id.*
21. *Securities Exchange Commission v. W.J. Howey, Co.*, 328 U.S. 293 (1946).
22. SEC Chairman Jay Clayton, Testimony on Virtual Currencies: *The Roles of the SEC and CFTC*, Before the Committee on Banking, Housing, and Urban Affairs, United States Senate (Feb. 6, 2018) (stating “[B]y and large, the structures of ICOs that I have seen involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws.”),

- available at:* <https://www.sec.gov/news/testimony/testimony-virtual-currencies-over-sight-role-us-securities-and-exchange-commission> (last visited Sep. 23, 2020). The Chairman also stated in response to questions from a Senator at the same hearing, “I believe *every* ICO I’ve seen is a security”. *Id.*
23. Section 202(a)(11) of the Advisers Act.
 24. Rule 206(4)-2.
 25. Rule 206(4)-2(d)(2).
 26. Rule 206(4)-2(d)(2); *see also* SEC Division of Investment Management Guidance Update 2017-01, *Inadvertent Custody: Advisory Contract Versus Custodial Contract Authority* (2017) (“2017 Guidance”), *available at:* <https://www.sec.gov/investment/im-guidance-2017-01.pdf> (last visited Sep. 23, 2020).
 27. *Id.*
 28. Rule 206(4)-2.
 29. Rule 206(4)-2(d)(6).
 30. Rule 206(4)-2(d)(6)(i); *see also* 15 U.S.C. § 80b–2. There is a tenable argument that a state-chartered trust company is a bank for purposes of the Custody Rule.
 31. Rule 206(4)-2(a)(3).
 32. Rule 206(4)-2(b)(2). The staff has issued guidance indicating that it would not “object” if an adviser to a pooled investment vehicle that is subject to an audit in accordance with paragraph (b)(4) of the rule does not maintain private stock certificates with a qualified custodian under certain circumstances that suggest that loss of the certificate will not adversely affect the pooled investment vehicle. *See* IM Guidance Update 2013-04 (Aug. 2013).
 33. *Engaging on Non-DVP Custodial Practices and Digital Assets*, SEC Division of Investment Management (Mar. 12, 2019), *available at:* https://www.sec.gov/investment/non-dvp-and-custody-digital-assets-031219-206#_edn1 (last visited Sep. 23, 2020).
 34. 2017 Guidance.
 35. Staff Letter: *Engaging on Fund Innovation and Cryptocurrency-related Holdings to Paul Schott Stevens, President & CEO, Investment Company Institute and Timothy W. Cameron, Asset Management Group – Head, Securities Industry and Financial Markets Association, from Dalia Blass, Director, Division of Investment Management*, U.S. Securities and Exchange Commission, Jan. 18, 2018, *available at:* <https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm> (last visited Sep. 23, 2020).
 36. *Id.*
 37. *See* SEC Staff Letter from *Dalia Blass, Director of SE Division of Investment Management, to Paul Schott Stevens, President & CEO, Inv. Co. Inst., & Timothy W. Cameron, Asset Mgmt. Grp.–Head, SIFMA* (Jan. 18, 2018), *available at:* <https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm> (last visited Sep. 23, 2020).
 38. *See* Rule 15c3-3(b)&(c). Whether an entity is a good control location is based on its ability to maintain exclusive control over customer securities. *See, e.g.,* Rule 15c3-3(c)(5) (recognising a “bank” as defined in Section 3(a)(6) of the Exchange Act as a good control location so long as, among other things, the bank has acknowledged that customer securities “are not subject to any right, charge, security interest, lien or claim of any kind in favor of a bank or any person claiming through the bank” and the securities are in the custody or control of the bank).
 39. *See* Rule 15c3-3(c)(1)&(5).

40. The SEC often receives applications under Rule 15c3-3(c)(7) to designate an issuer or the transfer agent of various types of uncertificated securities as a control location. The SEC Division of Trading and Markets has delegated authority to “find and designate as control locations for purposes of Rule 15c3-3(c)(7) certain broker-dealer accounts which are adequate for the protection of customer securities”. See 17 CFR 200.30-3(a)(10)(i). See also letter to Fantex Brokerage Services, LLC from Mark M. Attar, Senior Special Counsel, Division of Trading and Markets, SEC (Dec. 19, 2014) (providing that the staff would not recommend enforcement action if a broker-dealer treats a transfer agent for uncertificated securities as a good control location, under certain circumstances). The no-action letters do not address whether the use of blockchain technology, in connection with the maintenance of the single master security holder list, establishes control of uncertificated securities by the issuer (or transfer agent).
41. *Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities*, Division of Trading and Markets, SEC Office of General Counsel and Financial Industry Regulatory Authority (July 8, 2019) (the “Joint Statement”), available at: <https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities> (last visited Sep. 23, 2020). See also *Financial Industry Regulatory Authority – ATS Role in the Settlement of Digital Asset Security Trades*, SEC No-Action Letter (Sep. 25, 2020) (granting no action relief to FINRA for a three-step model for the settlement of transactions in digital asset securities), available at: <https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf> (last visited Sep. 23, 2020).
42. An ATS is a trading system that meets the definition of an “exchange” under federal securities laws that is not required to register as a national securities exchange if the ATS complies with the conditions to the exemption provided under Rule 3a1-1(a)(2) of the Exchange Act. See 17 CFR 242.300(a) (defining an alternative trading system) and CFR 242.3a1-1(a)(2) (the exemption from the definition of an exchange for an ATS). An ATS that is required to comply with Regulation ATS must register with the SEC as a broker-dealer. See 17 CFR 242.301(b)(1).
43. Joint Guidance.
44. See, e.g., Statement on Digital Asset Securities.
45. SEC, *What We Do* (June 10, 2013), available at: <https://www.sec.gov/Article/whatwedo.html> (last visited Sep. 23, 2020) and FINRA, *What We Do*, available at: <https://www.finra.org/about/what-we-do> (last visited Sep. 23, 2020).
46. See Rule 15c3-3(b)&(c). An entity’s designation as a good control location is based, in part, on its ability to maintain exclusive control over customer securities. See, e.g., Rule 15c3-3(c)(5).
47. See Rule 15c3-3(c)(1)&(c)(5).
48. Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers, OCC Interpretive Letter #1170 (Jul. 2020) (“OCC letter”), available at: <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf>.
49. *Id.* at 6–7.
50. *Id.* at 8.
51. *Id.*
52. See Section 17(f)(1) of the Investment Company Act, 15 USC § 80a-17(f)(1), and the rules thereunder. Following the OCC letter, the staff of the SEC Strategic Hub for Innovation and Financial Technology (“FinHub Staff”) issued a statement noting

the OCC has issued a limited interpretation regarding holding reserves of a stablecoin associated with hosted wallets that is backed by a single fiat currency and redeemable by the holder of the stablecoin on a 1:1 basis for the underlying fiat currency upon submission of a redemption request to the issuer. The FinHub staff reminded firms that whether a digital asset is a security under the federal securities laws is based on a facts and circumstances analysis. *SEC FinHub Staff Statement on OCC Interpretation* (Sep. 21, 2020), available at: <https://www.sec.gov/news/public-statement/sec-finhub-statement-occ-interpretation> (last visited Sep. 23, 2020).

53. Rule 15c3-3.
54. Louisiana recently joined New York and became the second state to enact a stand-alone virtual currency law. Louisiana’s Virtual Currency Business Act became effective August 1, 2020. For a comparison with the New York BitLicense, see Timothy C. Brown and Caroline L. Cordell, *Louisiana Serves Up New Virtual Currency Business Law Cajun Style*, *The National Law Review* (July 30, 2020), available at: <https://www.natlawreview.com/article/louisiana-serves-new-virtual-currency-business-law-cajun-style> (last visited Sep. 23, 2020).
55. N.Y. COMP. CODES R. & REGS. tit. 23, pt. 200 Virtual Currencies.
56. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.2(p).
57. “Exchange Service” means “the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency”. *Id.* § 200.2(d).
58. *Id.* § 200.2(q).
59. *Id.*
60. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.3(c).
61. See BitLicense Frequently Asked Questions, N.Y. State Department of Financial Services, available at: https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_faqs (last visited Sep. 23, 2020).
62. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.3(c).
63. *Organization of a Trust Company for the Limited Purpose of Exercising Fiduciary Powers*, N.Y. State Department of Financial Services, available at: <https://www.dfs.ny.gov/banking/iaus1a.htm> (last visited Sep. 23, 2020).



Richard B. Levin

Tel: +1 303 583 8261 / Email: rlevin@polsinelli.com

Richard B. Levin is the Chair of the FinTech and Regulation Practice at Polsinelli PC. His practice focuses on the representation of companies in the FinTech industry, including broker-dealers, hedge funds, alternative trading systems (ATSS), exchanges, and digital asset trading platforms. He represents these firms before the U.S. Securities and Exchange Commission, the U.S. Commodity Futures Trading Commission, the Financial Industry Regulatory Authority, and Congress. Richard has also represented clients before regulators around the world. *Chambers and Partners* has recognised him as a trusted adviser in the FinTech, blockchain, and cryptocurrency space. He is a frequent speaker at conferences on FinTech and regulatory issues and is the co-author of several chapters of books on U.S. regulation of digital assets and blockchain technology.



David M. Allred

Tel: +1 720 931 1193 / Email: dallred@polsinelli.com

David M. Allred is a shareholder with Polsinelli PC in the FinTech and Regulation and Securities Practices. He represents FinTech firms, banks, credit unions, finance companies, money service businesses (MSBs), non-bank lenders, third-party payment processors, prepaid card programmes, and alternative payment systems. David advises these firms in all stages of the business cycle. He helps clients confront complex regulatory matters including state and federal licensing, securities compliance, and corporate issues. David has served these firms on a range of complex legal issues including M&A, general corporate, regulatory compliance, securities, public and private offerings, and formations. He represents leading digital asset firms before the Financial Crimes Enforcement Network, the U.S. Securities and Exchange Commission, and state banking regulators. He has helped clients obtain exemptions from registration as an MSB in over 20 states. David is a certified public accountant.



Peter F. Waltz

Tel: +1 303 583 8254 / Email: pwaltz@polsinelli.com

Peter F. Waltz is a shareholder with Polsinelli PC in the FinTech and Regulation and Securities Practices. Peter focuses on securities and M&A in the FinTech industry, with particular emphasis on capital formation, securities compliance, and corporate governance matters. He also advises clients on securities regulatory issues before the U.S. Securities and Exchange Commission, the U.S. Commodity Futures Trading Commission, and the Financial Industry Regulatory Authority with a focus on investment advisers, private funds, broker-dealers, and alternative trading systems. Peter is a leader of Polsinelli's FinTech and Regulation Practice and has been recognised by *Chambers and Partners* as a trusted adviser in the FinTech space. Peter is a speaker at conferences on FinTech and regulatory issues and is the co-author of several chapters of books on U.S. regulation of digital assets and blockchain technology.

Polsinelli PC

1401 Eye ("I") Street, N.W., Suite 800, Washington, D.C. 20005, USA

Tel: +1 303 583 8261 / URL: www.polsinelli.com

Australia

Peter Reeves & Emily Shen
Gilbert + Tobin

Government attitude and definition

The developments in the local financial technology (**fintech**) landscape have propelled Australia as a leader in this sector. Australia is generally perceived to be a stable jurisdiction that is relatively fintech-friendly and this perception has been facilitated by a broad range of product offerings from the Australian fintech community and the commitment to facilitate growth and innovation in the sector by the Commonwealth Government of Australia (**Government**). While there has been increased regulatory involvement particularly following the completion of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in 2019 (**Royal Commission**), fintechs have seen a unique opportunity to develop and position themselves in Australia's economy. In part, the expansion of the sector in Australia has been led by businesses in the payments, lending, investment and custodial services spaces.

To date, the Government has taken a largely non-interventionist approach to the regulation of cryptocurrency, allowing the landscape to evolve at a faster rate than its regulatory response. Australian law does not currently equate digital currency with fiat currency and does not treat cryptocurrency as “money”.

The Governor of the Reserve Bank of Australia (**RBA**), Australia's central bank, has confirmed that the RBA has no immediate plans to issue a digital dollar akin to money. Terming it an “eAUD”, the Governor noted that the rise of new technology associated with cryptocurrencies has the capacity to challenge the role of traditional financial institutions with regard to payments, but that there is currently no public policy case for the RBA to issue an eAUD. Despite this, the Governor indicated that the RBA remains open to considering wholesale applications for a digital Australian dollar and would be continuing to research this area with ongoing studies of the use of a central bank-issued digital dollar in relation to settlement arrangements.

While the Government has not significantly intervened in cryptocurrencies and related activities, there has been general clarification of the application of Australian regulatory regimes to the sector. For example, the Government passed the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* (**AML/CTF Amendment Act**), which brought cryptocurrencies and tokens within the scope of Australia's anti-money laundering regime. This recognised the movement towards digital currencies becoming a popular method of paying for goods and services and transferring value in the Australian economy, but also posing significant money laundering and terrorism financing risks.

Cryptocurrency regulation

While there have been legislative amendments to accommodate the use of cryptocurrencies, these have predominantly focused on the transactional relationships (e.g., the issuing and exchanging process) and activities involving cryptocurrencies, rather than the cryptocurrencies themselves.

Australia's primary corporate, markets, consumer credit and financial services regulator, the Australian Securities and Investments Commission (ASIC), has reaffirmed the view that legislative obligations and regulatory requirements are technology-neutral and apply irrespective of the mode of technology that is being used to provide a regulated service. While there has been no legislation created to deal with cryptocurrencies as a discrete area of law, this does not hinder them from being captured within existing regimes under Australian law.

ASIC's regulatory guidance informs businesses of ASIC's approach to the legal status of coins (or tokens). The legal status of such coins is dependent on how they are structured and the rights attached, which ultimately determines the regulations with which an entity must comply. For example:

- Cryptocurrency that is characterised as a financial product under the *Corporations Act 2001* (Cth) (**Corporations Act**) will fall within the scope of Australia's existing financial services regulatory regime. This is discussed in more detail under "Sales regulation" below.
- There has also been a proliferation of lending activities in relation to cryptocurrency. To the extent these lending activities fall within the scope of the credit activities and services caught under the *National Credit Consumer Protection Act 2009* (Cth) (**NCCP Act**), the relevant entities may need to hold an Australian credit licence or be otherwise exempt from the requirement to be licensed.

There are currently no specific regulations dealing with blockchain or other distributed ledger technology (DLT) in Australia. However, in March 2017, ASIC released an information sheet (*INFO 219 Evaluating distributed ledger technology*) outlining its approach to the regulatory issues that may rise through the implementation of blockchain technology and DLT solutions more generally. Businesses considering operating market infrastructure, or providing financial or consumer credit services using DLT, will still be subject to the compliance requirements that currently exist under the applicable licensing regime. There is a general obligation that entities relying on technology in connection with the provision of a regulated service must have the necessary organisational competence and adequate technological resources and risk-management plans in place. While the existing regulatory framework is sufficient to accommodate current implementations of DLT, as the technology matures, additional regulatory considerations will arise.

Various cryptocurrency networks have also implemented "smart" or self-executing contracts. These are permitted in Australia under the *Electronic Transactions Act 1999* (Cth) (**ETA**) and the equivalent Australian state and territory legislation. The ETA provides a legal framework to enable electronic commerce to operate in the same way as paper-based transactions. Under the ETA, self-executing contracts are permitted in Australia, provided they meet all the traditional elements of a legal contract.

Sales regulation

The sale of cryptocurrency and other digital assets is regulated by Australia's existing financial services regulatory regime. Core considerations for issuers are outlined below.

Licensing

Of particular concern to those dealing with cryptocurrencies is whether a cryptocurrency (including those offered during an initial coin offering (ICO)) constitutes a financial product and therefore triggers financial services licensing and disclosure requirements. Entities carrying on a financial services business in Australia must hold an Australian financial services licence (AFSL) or be exempt. The definitions of “financial product” or “financial service” under the Corporations Act are broad and ASIC has indicated in its information sheet, *INFO 225 Initial coin offerings (INFO 225)*, that cryptocurrency with similar features to existing financial products or securities will trigger the relevant regulatory obligations.

In INFO 225, ASIC indicated that the legal status of cryptocurrency is dependent upon the structure of the ICO and the rights attaching to the coins or tokens. ASIC has also indicated that what is a right should be interpreted broadly. Depending on the circumstances, coins or tokens may constitute interests in managed investment schemes (collective investment vehicles), securities, derivatives, or fall into a category of more generally defined financial products, all of which are subject to the Australian financial services regulatory regime. In INFO 225, ASIC has provided high-level regulatory signposts for crypto-asset participants to determine whether they have legal and regulatory obligations. These signposts are relevant to crypto-asset issuers, crypto-asset intermediaries, miners and transaction processors, crypto-asset exchanges and trading platforms, crypto-asset payment and merchant service providers, wallet providers and custody service providers, and consumers.

Broadly, entities offering coins or tokens that can be classified as financial products will need to comply with the regulatory requirements under the Corporations Act which generally include disclosure, registration, licensing and conduct obligations. An entity that facilitates payments by cryptocurrencies may also be required to hold an AFSL and the operator of a cryptocurrency exchange may be required to hold an Australian market licence if the coins or tokens traded on the exchange constitute financial products.

Generally, ASIC’s regulatory guidance is consistent with the position of regulators in other jurisdictions. ASIC has also recommended that companies wishing to conduct an ICO or other token sale seek professional advice, including legal advice, and contact its Innovation Hub (discussed in detail below, “Promotion and testing”) for informal assistance. This reflects its willingness to build greater investor confidence around cryptocurrency as an asset class. However, ASIC has emphasised consumer protection and compliance with the relevant laws and has taken action as a result to stop proposed ICOs targeting retail investors due to issues with disclosure and promotional materials (the requirements of which are discussed below) as well as offerings of financial products without an AFSL.

In 2019, the Treasury consulted on ICOs and the relevant regulatory frameworks in Australia; however, no outcomes of this consultation have been reported to date.

Marketing

ASIC’s recognition that a token sale may involve an offer of financial products has clear implications for the marketing of the token sale. For example, an offer of a financial product to a retail client (with some exceptions) must be accompanied by a regulated disclosure document (e.g., a product disclosure statement or a prospectus and a financial services guide) that satisfies the content requirements of the Corporations Act and regulatory guidance published by ASIC. Such a disclosure document must set out prescribed information, including the provider’s fee structure, to assist a client to decide whether to acquire the cryptocurrency from the provider. In some instances, the marketing activity itself may cause the token sale to be an offer of a regulated financial product.

Under the Corporations Act, depending on the minimum amount of funds invested per investor and whether the investor is a “sophisticated investor” or wholesale client, an offer of financial products may not require regulated disclosure.

Cross-border issues

Carrying on a financial services business in Australia will require a foreign financial services provider (**FFSP**) to hold an AFSL, unless relief is granted. Entities, including FFSPs, should note that the Corporations Act may apply to an ICO or token sale regardless of whether it was created and offered from Australia or overseas. Currently, Australia has a foreign AFSL (**FAFSL**) regime for FFSPs regulated in certain jurisdictions that enables FFSPs regulated in those jurisdictions to provide financial services in Australia without holding an AFSL. To be eligible, the FFSP must be authorised under an overseas regulatory regime that ASIC has assessed as sufficiently equivalent to the Australian regulatory regime (currently including Denmark, France, Germany, Hong Kong, Luxembourg, Ontario in Canada, Singapore, Sweden, the United Kingdom, and the United States of America). However, holding a FAFSL will only cover the provision of services to wholesale clients (similar to the concept of an accredited investor under US law), and the FFSP must only provide the services it is authorised to provide in its home jurisdiction. The FAFSL regime replaces the previous passporting arrangements Australia had in place (though FFSPs already relying on passport relief may do so until 31 March 2022).

Foreign companies taken to be carrying on a business in Australia, including by issuing cryptocurrency or operating a platform developed using ICO proceeds, may be required to either establish a local presence (i.e., register with ASIC and create a branch) or incorporate a subsidiary. Broadly, the greater the level of system, repetition or continuity associated with an entity’s business activities in Australia, the greater the likelihood that registration will be required. Generally, a company holding an AFSL will be carrying on a business in Australia and will trigger the requirement.

Promoters should also be aware that if they wish to market their cryptocurrency to Australian residents, and the coins or tokens are considered a financial product under the Corporations Act, they will not be permitted to market the products unless the requisite licensing and disclosure requirements are met. Generally, a service provider from outside of Australia may respond to requests for information and issue products to an Australian resident if the resident makes the first (unsolicited) approach and there has been no conduct on the part of the issuer designed to induce the investor to make contact, or activities that could be misconstrued as the provider inducing the investor to make contact.

Design and distribution obligations and product intervention powers

The *Treasury Laws Amendment (Design and Distribution Obligations and Product Intervention Powers) Act 2019* (Cth) (**DDO PIP Act**) and Corporations Amendment (Design and Distribution Obligations and Product Intervention Powers) Regulations 2018 may also impact the way cryptocurrencies are structured and token sales are conducted in the future. The DDO PIP Act introduces new design and distribution obligations in relation to financial products and provides ASIC with temporary product intervention powers where there is a risk of significant consumer detriment. The new arrangements aim to ensure that financial products are targeted at the correct category of potential investors. ASIC has released regulatory guidance on its product intervention powers, stating that the power enables ASIC to address market-wide problems or specific business models and deal with “first mover” issues causing consumer detriment. The power covers financial products under the Corporations Act and *Australian Securities and Investments Commission Act*

2001 (Cth) (**ASIC Act**) and credit products under the NCCP Act. These powers are highly likely to impact marketing and distribution practices in the cryptocurrency sector where cryptocurrencies fall within the remit of the powers.

Consumer law

Even if a token sale is not regulated under the Corporations Act, it may still be subject to other regulation and laws, including the Australian Consumer Law set out at Schedule 2 to the *Competition and Consumer Act 2010* (Cth) (**ACL**) relating to the offer of services or products to Australian consumers. The ACL prohibits misleading or deceptive conduct in a range of circumstances, including in the context of marketing and advertising. As such, care must be taken in token sale promotional material to ensure that buyers are not misled or deceived and that the promotional material does not contain false information. In addition, promoters and sellers are prohibited from engaging in unconscionable conduct and must ensure the coins or tokens issued are fit for their intended purpose.

The protections of the ACL are generally reflected in the ASIC Act, providing substantially similar protection to investors in financial products or services.

ASIC has also received delegated powers from the Australian Competition and Consumer Commission to enable it to take action against misleading or deceptive conduct in marketing or issuing token sales (regardless of whether it involves a financial product). ASIC has indicated misleading or deceptive conduct in relation to token sales may include:

- using social media to create the appearance of greater levels of public interest;
- creating the appearance of greater levels of buying and selling activity for a token sale or a crypto-asset by engaging in (or arranging for others to engage in) certain trading strategies;
- failing to disclose appropriate information about the token sale; or
- suggesting that the token sale is a regulated product or endorsed by a regulator when it is not.

ASIC has stated that it will use this power to issue further inquiries into token issuers and their advisers to identify potentially unlicensed and misleading conduct.

A range of consequences may apply for failing to comply with the ACL or the ASIC Act, including monetary penalties, injunctions, compensatory damages and costs orders.

Taxation

The taxation of cryptocurrency in Australia has been an area of much debate, despite recent attempts by the Australian Taxation Office (**ATO**) to clarify the operation of the tax law. For income tax purposes, the ATO views cryptocurrency as an asset that is held or traded (rather than as money or a foreign currency).

Holders of cryptocurrencies

The tax implications for holders of cryptocurrency depends on the purpose for which the cryptocurrency is acquired or held. The summary below applies to holders who are Australian residents for tax purposes.

If a holder of cryptocurrency is carrying on a business that involves transacting in a cryptocurrency, the cryptocurrency will be held as trading stock. Gains on the sale of the cryptocurrency will be assessable and losses will be deductible (subject to integrity measures and “non-commercial loss” rules). Examples of relevant businesses include cryptocurrency trading and cryptocurrency mining businesses.

Whether or not a taxpayer's activities amount to carrying on a business is a question of fact and degree, and is ultimately determined by weighing up the taxpayer's individual facts and circumstances. Generally (but not exclusively), where the activities are undertaken for a profit-making purpose, are repetitious, involve ongoing effort, and include business documentation, the activities would amount to the carrying on of a business.

Even if a holder of cryptocurrency did not invest or acquire the cryptocurrency in the ordinary course of carrying on a business, profits or gains from an "isolated transaction" involving the sale or disposal of cryptocurrency may still be assessable where the transaction was entered into with a purpose or intention of making a profit, and the transaction was part of a business operation or commercial transaction.

If cryptocurrency is not acquired or held in the course of carrying on a business, or as part of an isolated transaction with a profit-making intention, a profit on sale or disposal should be a capital gain. In this regard, the ATO has indicated that cryptocurrency is a capital gains tax (CGT) asset. Capital gains may be discounted under the CGT discount provisions, so long as the taxpayer satisfies the conditions for the discount (that is, the cryptocurrency is held for at least 12 months before it is disposed of).

Although cryptocurrency may be a CGT asset, a capital gain arising on its disposal may be disregarded if the cryptocurrency is a "personal use asset" and it was acquired for A\$10,000 or less. Capital losses made on cryptocurrencies that are personal use assets are also disregarded. Cryptocurrency will be a personal use asset if it was acquired and used within a short period of time for personal use or consumption (that is, to buy goods or services).

Note that the ATO's views on the income tax implications of transactions involving cryptocurrencies is in a state of flux due to the rapid evolution of both cryptocurrency technology and its uses.

Issuers of cryptocurrencies

In the context of an ICO, a coin issuance by an entity that is either an Australian tax resident, or acting through an Australian "permanent establishment", may be assessable in Australia. The current corporate tax rate in Australia is either 26% or 30%. However, if the issued coins are characterised as equity for tax purposes or are issued in respect of a borrowing of money, the ICO proceeds may not be assessable to the issuer.

Australian Goods and Services Tax (GST)

Supplies and acquisitions of digital currency made from 1 July 2017 are not subject to GST on the basis that they will be input-taxed financial supplies. Consequently, suppliers of digital currency will not be required to charge GST on these supplies, and a purchaser would *prima facie* not be entitled to GST refunds (i.e., input tax credits) for these corresponding acquisitions. On the basis that digital currency is a method of payment, as an alternative to money, the normal GST rules apply to the payment or receipt of digital currency for goods and services.

The term "digital currency" in the GST legislation requires that it is a digital unit of value that has all the following characteristics:

- it is fungible and can be provided as payment for any type of purchase;
- it is generally available to the public free of any substantial restrictions;
- it is not denominated in any country's currency;
- the value is not derived from or dependent on anything else; and
- it does not give an entitlement or privileges to receive something else.

In relation to a holder carrying on a business of cryptocurrency mining, whether or not GST is payable by the miner on its supply of new cryptocurrency depends on a number of

factors, including its specific features, whether the miner is registered for GST, and whether the supply is made in the course of the miner's enterprise.

The specific features of cryptocurrency include it: being a type of security or other derivative; being "digital currency" as defined in the GST legislation; or providing a right or entitlement to goods or services. If the cryptocurrency is "digital currency", its supply will not be subject to any GST because it will be an input-taxed financial supply (assuming the other requirements are satisfied).

A cryptocurrency miner would generally be required to register for GST if its annual GST turnover is A\$75,000 or more, excluding the value of its supplies of digital currencies and other input-taxed supplies. However, a miner who does not satisfy this GST registration threshold may nevertheless elect to register for GST in order to claim from the ATO full input tax credits (i.e., GST refunds) for the GST cost of its business acquisitions (but acquisitions that relate to the sales or acquisitions of digital currencies are *prima facie* non-creditable or non-refundable).

Enforcement

The ATO has created a specialist task force to tackle cryptocurrency tax evasion. The ATO also collects bulk records from Australian cryptocurrency designated service providers to conduct data matching to ensure that cryptocurrency users are paying the right amount of tax. With the broader regulatory trend around the globe moving from guidance to enforcement, it is likely that the ATO will also begin enforcing tax liabilities more aggressively.

Money transmission laws and anti-money laundering requirements

In 2017, the Government passed the AML/CTF Amendment Act, which brought cryptocurrencies and tokens within the scope of Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regulatory framework. The amendments came into force on 3 April 2018 and focus on the point of intersection between cryptocurrencies and the regulated financial sector, namely digital currency exchanges (DCEs).

Broadly, DCE providers are now required to register with the Australian Transaction Reports and Analysis Centre (AUSTRAC) to operate, with a penalty of up to two years' imprisonment or a fine of up to A\$111,000, or both, for failing to register. Registered exchanges will be required to implement know-your-customer processes to adequately verify the identity of their customers, with ongoing obligations to monitor and report suspicious and large transactions. Exchange operators are also required to keep certain records relating to customer identification and transactions for up to seven years.

Promotion and testing

Regulators in Australia have generally been receptive to fintech and innovation and have sought to improve their understanding of, and engagement with, businesses by regularly consulting with industry on proposed regulatory changes. While there are no programmes specifically promoting research and investment in cryptocurrency, both ASIC and AUSTRAC have established Innovation Hubs designed to assist fintech businesses more broadly in understanding their obligations under Australian law. ASIC has also entered into a number of cooperation agreements with overseas regulators, which aim to further understand the approach of fintech businesses in other jurisdictions (as discussed below).

ASIC Innovation Hub

The ASIC Innovation Hub is designed to foster innovation that could benefit consumers by helping Australian fintech start-ups navigate the Australian regulatory system. The

Innovation Hub provides tailored information and access to informal assistance intended to streamline the AFSL process for innovative fintech start-ups, which could include cryptocurrency-related businesses.

In December 2016, ASIC made certain class orders establishing a fintech licensing exemption allowing fintech businesses to test certain financial services, financial products and credit activities without holding an AFSL or Australian credit licence by relying on the class orders (referred to as the regulatory sandbox). There are strict eligibility requirements for both the type of businesses that can enter the regulatory sandbox and the products and services that qualify for the licensing exemption. There are restrictions on how many persons can be provided with a financial product or service, and caps on the value of the financial products or services that can be provided.

In 2020, the Government introduced an “enhanced regulatory sandbox”, which expands the scope of ASIC’s regulatory sandbox to test a broader range of financial services and credit activities for up to 24 months. This is intended to better support innovation in the sector. The enhanced regulatory sandbox has two eligibility tests that must be satisfied and there are caps on the value of financial services and exposure provided.

Cross-border business

Beyond this, ASIC has engaged with regulators overseas to deepen its understanding of innovation in financial services, including in relation to cryptocurrencies. In particular, ASIC and the United Kingdom’s Financial Conduct Authority have signed an Enhanced Cooperation Agreement, which allows the two regulators to, among other things, information-share, refer innovative businesses to each regulator’s respective regulatory sandbox, and conduct joint policy work. ASIC also currently has either information-sharing or cooperation agreements with regulators in jurisdictions such as Canada, Hong Kong, Indonesia, Kenya and Singapore. These arrangements facilitate the cross-sharing of information on fintech market trends, encourage referrals of fintech companies and share insights from proofs of concepts and innovation competitions.

ASIC is also a signatory to the IOSCO Multilateral Memorandum of Understanding, which has committed over 100 regulators to mutually assist and cooperate with each other, particularly in relation to the enforcement of securities laws.

ASIC has committed to supporting financial innovation in the interests of consumers by joining the Global Financial Innovation Network (**GFIN**), which was formally launched in January 2019 by a group of financial regulators across 29 member organisations. The GFIN is dedicated to facilitating regulatory collaboration in a cross-border context and provides more efficient means for innovative businesses to interact with regulators.

In 2019, a group of fintech associations formed the Asia-Pacific FinTech Network, which is designed to facilitate greater collaboration, cooperation and innovation across the region. The network will focus on sectors including RegTech, Blockchain, Payment Systems, Artificial Intelligence and Financial Inclusion and is expected to accelerate fintech development and lower financial costs both domestically and internationally.

AUSTRAC Innovation Hub

AUSTRAC’s Fintel Alliance is a private-public partnership seeking to develop “smarter regulation”. This includes setting up an innovation hub targeted at improving the fintech sector’s relationship with the Government and regulators. The hub will provide a regulatory sandbox for fintech businesses to test financial products and services without risking regulatory action or costs.

Ownership and licensing requirements

At the time of writing, there are currently no explicit restrictions on investment managers owning cryptocurrencies for investment purposes. However, investment managers may be subject to Australia's financial services regulatory regime where the cryptocurrencies held are deemed to be "financial products" and the investment managers' activities in relation to those cryptocurrencies are deemed to be the provision of financial services.

For example, investment managers providing investment advice on cryptocurrencies held that are financial products will be providing financial product advice under the Corporations Act and must hold an AFSL or otherwise be exempt from the requirement to be licensed. ASIC has provided significant guidance in relation to complying with the relevant advice, conduct and disclosure obligations, as well as the conflicted remuneration provisions under the Corporations Act. Further, investment managers may be required to hold an AFSL with a custodial or depository authorisation or be exempt from this requirement if investment managers wish to custody cryptocurrencies that are financial products on behalf of clients.

Australia has also seen a rapidly rising interest in robo-advice or digital advice models. The provision of robo-advice is where algorithms and technology provide automated financial product advice without a human advisor. For investment or fund businesses seeking to operate in Australia by providing digital or hybrid advice (including with respect to investing in cryptocurrencies), there are licensing requirements under the Corporations Act. ASIC has released *Regulatory Guide 255: Providing digital financial product advice to retail clients*, which details issues that digital advice providers need to consider generally, during the AFSL application stage and when providing digital financial product advice to retail clients. It is intended to complement ASIC's existing guidance including *Regulatory Guide 36: Licensing: Financial product advice and dealing*. Financial product advisers also need to consider their conduct and disclosure obligations. ASIC has released *Regulatory Guide 175: Licensing: Financial product adviser – conduct and disclosure* with respect to this.

Mining

At the time of writing, there are no prohibitions on mining Bitcoin or other cryptocurrencies in Australia.

Cryptocurrency mining taxation

As above, the taxation of cryptocurrency and associated activities in Australia has been an area of much debate, and this has extended to taxation relating to mining cryptocurrency. See "Taxation" above for further information.

Cybersecurity

More generally, with the rise of cloud-based Bitcoin mining enterprises in Australia, mining businesses should carefully consider cybersecurity issues in relation to mining activities.

In its Corporate Plan 2020 to 2024, ASIC stated that a key priority was to improve management of key risks and that, partly as a result of the COVID-19 pandemic, entities "without appropriate systems in place are increasingly vulnerable to cyber attacks, data breaches, technology failures and system outages". CERT Australia (now part of the Australian Cyber Security Centre) noted that there has been an increase in cryptomining malware affecting businesses' resources and processing capacity.

ASIC has also released regulatory guidance to help firms improve their cyber resilience, including reports, articles and practice guides. Most recently, ASIC has released Report 651 *Cyber Resilience of firms in Australia's financial markets: 2018–19*, which identifies

key trends in cyber resilience practices and highlights existing good practices and areas for improvement. ASIC has previously provided two reports, namely Report 429 *Cyber resilience: Health check* and Report 555 *Cyber resilience of firms in Australia's financial markets*, which examine and provide examples of good practices identified across the financial services industry. The reports contain questions that board members and senior management of financial organisations should ask when considering cyber resilience.

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings when entering or leaving Australia.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act)* mandates that both individuals and businesses must submit reports where physical currency in excess of A\$10,000 (or foreign currency equivalent) is brought into or taken out of Australia. This requirement is restricted to “physical currency”, which AUSTRAC has defined as being any coin or printed note of Australia or a foreign country that is designated as legal tender, and is circulated, customarily used and accepted as a medium of exchange in the country of issue. Although market commentary indicates that some governments have created or are attempting to issue official cryptocurrencies, the intangible nature of cryptocurrency remains a bar to cryptocurrency being captured by declaration obligations under the AML/CTF Act for the time being.

It should be noted that the AML/CTF Act was amended to address some aspects of cryptocurrency transfer and exchange; however, this amendment did not see the scope of AML/CTF regulation widen the border restrictions. At the time of writing, there appears to be no indication that any such further amendment to include border restrictions is being contemplated.

Reporting requirements

The AML/CTF Act imposes obligations on entities that provide certain “designated services” with an Australian connection. Generally, the AML/CTF Act applies to any entity that engages in financial services or credit (consumer or business) activities in Australia, including the provision of DCE services. These obligations include record-keeping and reporting requirements.

For example, the AML/CTF Rules outline reportable details for matters including, but not limited to, threshold transaction reports (**TTRs**). TTRs will be required to be submitted where transactions over A\$10,000 have occurred. Reportable information includes, among other details, the denomination or code of the digital currency and the value of digital currency expressed in Australian dollars (if known), a description of the digital currency including details of the backing asset or thing (if known), the Internet Protocol address information, email address, mobile phone and social media identifiers of the payee and recipient, name of the recipient, address and date of birth of the recipient (if known), and the unique identifiers relating to the digital currency wallet of the payee and recipient as well as the unique device identifiers of the payee and recipient.

In April 2016, the Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations (**AML/CTF Report**), which contained 84 recommendations to improve Australia's AML/CTF regime, was released. The AML/CTF Report contemplated two phases of consultation and

implementation, with Phase 1 including priority projects completed in 2017, while Phase 2 progresses major, long-term reforms. These reforms should, among other things, clarify record-keeping requirements and reporting obligations for reporting entities.

Estate planning and testamentary succession

To date, there has been no explicit regulation or case law surrounding the treatment of cryptocurrency in Australian succession law. Generally, if estate plans do not cater for the specific nature of cryptocurrency and steps are not taken to ensure executors can access a deceased's cryptocurrency (e.g., by accessing the private key), it may not pass to the beneficiaries.

A will should be drafted to give the executor authority to deal with digital assets. It may be helpful to select an executor with some knowledge of or familiarity with cryptocurrencies. As cryptocurrencies are generally held anonymously, a will should also establish the existence of the cryptocurrency as an asset to be distributed to beneficiaries. A method must also be established to ensure passwords to digital wallets and external drives storing cryptocurrency are accessible by a trusted representative. Unlike a bank account which can be frozen upon death, anyone can access a digital wallet, so care should be taken to ensure external drives and passwords are not easily accessible on the face of the will. This may include providing a memorandum of passwords and accounts to the executor to be placed in a safe custody facility which remains unopened until a will is called upon.

There may also be tax implications arising for the beneficiaries of cryptocurrencies, which are similar to the tax implications for cryptocurrency holders. See "Taxation" above for further details.

**Peter Reeves****Tel: +61 2 9263 4290 / Email: preeves@gtlaw.com.au**

Peter is a partner in Gilbert + Tobin's Corporate Advisory group and leads the Fintech practice at G+T. He is an expert and market-leading practitioner in fintech and financial services regulation. Peter advises domestic and offshore corporates, financial institutions, funds, managers and other market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. He also advises across a range of issues relevant to the fintech and digital sectors, including platform structuring and establishment, payments, blockchain solutions and digital asset strategies.

**Emily Shen****Tel: +61 2 9263 4402 / Email: eshen@gtlaw.com.au**

Emily is a lawyer in Gilbert + Tobin's Corporate Advisory group with a focus on Australian financial services regulation, funds management and fintech. She has been involved in advising a range of clients across the financial services, fintech and digital sectors on issues including platform and fund establishment, structuring tokenisation deployments, and implementing payment and blockchain solutions.

Gilbert + Tobin

Level 35, Tower Two, International Towers Sydney, 200 Barangaroo Avenue, Barangaroo, Sydney NSW 2000, Australia
Tel: +61 2 9263 4000 / URL: www.gtlaw.com.au

Austria

Ursula Rath & Thomas Kulnigg
Schönherr Rechtsanwälte GmbH

Government attitude and definition

Austrian financial regulators and policymakers are generally receptive to cryptocurrencies, new technologies and fintech.

The Austrian government closely monitors developments in the area of alternative means of financing through distributed ledger technology (“DLT”) and other digital assets, such as initial coin offerings (“ICOs”), initial token offerings (“ITOs”), security token offerings (“STOs”) and initial exchange offerings (“IEOs”), which, however, seem to have slowed down significantly over the last year and a half. On the other hand, we have noticed an uptick in innovative digital business models across a wide range of industries, including in the mobile payments services sector, and more generally in platform-based crowdfunding/ investment offerings.

To further strengthen innovation, the current Austrian governmental programme hopes to improve incentives for private venture capital for innovative start-ups and small- and medium-sized enterprises (“SMEs”). The trend appears to have moved away from using blockchain/ DLT as a financing instrument for start-ups to being used for more mature applications. In particular, financial institutions are increasingly interested in cryptoassets and blockchain/ DLT applications in Austria.

The Austrian Financial Markets Authority (*Finanzmarktaufsicht*; “FMA”) has established a dedicated fintech contact point to assist with new business models requiring authorisation under Austrian financial services regulation (see further below).

At the same time, regulators and the government stress that integrity, security and investor protection must not be compromised. While Austrian law does not prohibit cryptocurrencies, the FMA has warned investors of the risks of cryptocurrencies, stating that virtual currencies like Bitcoin and trading platforms for such instruments are neither regulated nor supervised by the FMA.

Cryptocurrency regulation

In Austria, no cryptocurrencies or fintech-specific laws or regulations have currently been enacted. Although there is no statutory definition of cryptocurrencies, according to the Austrian regulator, the FMA, cryptocurrencies are typically characterised as follows:

- they are not issued by any central bank or governmental authority;
- new units of value are typically created using a predefined procedure within a computer network (commonly referred to as “mining”);
- there is no central authority that verifies or manages transactions;

- transactions are recorded on a decentralised, publicly held ledger (commonly referred to as “blockchain”) and, once executed, cannot be revoked; and
- electronic wallets may be used to store and manage virtual currencies (commonly referred to as “wallets”).

Furthermore, cryptocurrency is currently not treated as “money” or otherwise given equal status with domestic or foreign fiat currency in Austria. Likewise, there are not yet any cryptocurrencies that are backed by the Austrian government or the Austrian National Bank. From an Austrian financial services regulatory perspective, cryptocurrencies are currently neither treated as financial instruments (in particular, not as securities or derivatives) nor as currency (domestic or foreign), but as commodities. It is worth noting, however, that derivative instruments referencing cryptocurrencies or tokens will qualify as financial instruments under the second Markets in Financial Instruments Directive (“MiFID II”) and hence will be covered by financial services regulation under MiFID II and the Markets in Financial Instruments Regulation (“MiFIR”).

While commodities as such are not subject to supervision by the FMA, this does not mean that business activities involving cryptocurrencies are entirely outside the Austrian regulatory remit. Depending on their precise features/content, the operation of various business models based on cryptocurrencies may trigger licensing requirements under the Austrian Banking Act (*Bankwesengesetz*; “BWG”), the Austrian Alternative Investment Fund Managers Act (*Alternative Investmentfonds Manager-Gesetz*; “AIFMG”) or the Austrian Payment Services Act (*Zahlungsdienstegesetz*; “ZaDiG”), and/or prospectus requirements under the EU Prospectus Regulation or the Austrian Capital Markets Act (*Kapitalmarktgesetz*; “KMG”).

In this respect, the general legal framework also applies to cryptocurrencies and new technologies. The FMA is known to apply a “technology-neutral” supervisory approach, meaning that products and services are subject to the same regulatory framework as “traditional” products/services. The underlying rationale is “same risk – same rules”. If and to what extent financial services regulation applies, primarily depends on the actual product features/activities.

Innovative business models involving cryptocurrencies may be subject to licensing requirements and governed by:

- the BWG – for example, if funds are raised for investment into cryptocurrencies;
- the ZaDiG 2018 – for example, if information of several accounts is consolidated or if payments are initiated;
- the Securities Supervision Act 2018 – for example, if investment advice or portfolio management are provided in relation to financial instruments referencing cryptocurrencies or if orders are received and transmitted in relation to such instruments;
- the AIFMG – for example, if funds are raised for investment into cryptocurrencies according to a pre-defined investment strategy; and
- the Electronic Money Act – when issuing electronic money.

The FMA has published further guidance on the regulatory treatment of certain activities around cryptocurrencies, ICOs/ITOs and fintech on the fintech navigator section of its website at <https://www.fma.gv.at/en/cross-sectoral-topics/fintech/fintech-navigator/>.

Key areas to note are the following:

- Purely technical services do not require a licence under financial services regulation. If, however, a technical billing service also includes transfer of funds, this would no longer be considered a purely technical service and would need to be tested against licensing requirements under the BWG, the AIFMG and the Austrian Electronic Money Act.

- Alternative currencies, payment instruments or means of payment may trigger a licensing requirement if they are intended for payment at third parties, and the network within which they can be used to purchase goods/services is large in terms of geographical reach, type of products/services and/or number of accepting parties (there is a licensing exception for restricted networks, but this has become increasingly strict following the implementation of Directive 2015/2366/EU (“PSD II”). Also, if accounts are operated in connection with currencies, payment instruments or means of payment through which payments are made, the entity holding the accounts may be obliged to become licensed as a payment service provider.
- If capital is raised in order to invest proceeds into cryptocurrencies or mining, this could be regulated as a banking business (deposits business) or as managing an alternative investment fund (“AIF”) under the AIFMG if funds are invested in accordance with a defined investment strategy and returns in each case depend on the performance of the underlying investment. If the capital-raising is structured through the issuance of shares or similar participation in a corporation or partnership, this may also trigger prospectus requirements under Austrian securities laws (see “Sales regulation”, below).
- Online platforms for acquiring virtual currencies that also settle/process payments in domestic or foreign currency through their own accounts may require a licence under the AIFMG. Generally, if funds pass through the provider’s accounts, this will trigger a licence requirement under payment services regulations. Some online service providers therefore cooperate with licensed partners and transfer funds via their accounts.
- Brokers of new or alternative payment methods may need to become licensed if they are considering intermediating deposits or loans/insurance. This would be the case if an app or online platform was linked to a specific deposit/current account. The mere listing of product information, for example, via product comparison portals, would not require a licence.
- While merely buying and selling virtual currencies in one’s own name and for one’s own account generally does not trigger a licence requirement, the buying and selling of virtual currencies may form part of business models that do require a licence. For instance, the operation of a Bitcoin vending machine may trigger a licence requirement, depending on its features. Also, clearing a Bitcoin vending machine and subsequently transferring any funds collected to a third party may require a payment services licence for money remittance under the AIFMG.
- There is currently no deposit guarantee scheme and no legal investor protection scheme for cryptocurrencies or tokens.

Given the diversity, complexity and rapid evolution of business models in the fintech space, the regulatory treatment of any business models involving cryptocurrencies or tokens will need to be assessed on a case-by-case basis.

The FMA therefore encourages discussion of the regulatory treatment prior to engaging in any business activity. It has set up a dedicated specialist team and fintech contact portal dedicated to those areas, which handles all fintech-related queries.

Sales regulation

There is currently no specific regulation dedicated to the sale of cryptocurrencies or tokens, which are thus covered by general securities and commodities laws.

Depending on a token’s terms and conditions/features, certain token offerings/sales may be subject to prospectus requirements under Austrian securities laws unless a prospectus

exemption applies. Each offering must be assessed on a case-by-case basis and the regulatory assessment will depend on the specific technical, functional and economic design of the instruments offered.

For Austrian supervisory law purposes, the FMA has broadly classified tokens as set out below, noting that in practice, hybrid forms and overlaps frequently occur and that such classification is subject to any further national and international legal developments:

- Security/investment tokens: Tokens that represent assets, in particular payment claims against a specific issuer, e.g. to participate in future earnings or cash flows or tokens that represent membership rights within the meaning of corporate law. The design of such tokens is often similar to that of “classical securities”, in particular bonds or shares. Security tokens are therefore frequently considered transferable securities pursuant to the EU Prospectus Regulation and the Austrian Securities Supervision Act. If a token is classified as a transferable security, this has far-reaching regulatory implications not only for the token issuer (as this may trigger prospectus requirements under European securities laws) but also for trading platforms on which such token is traded (as they will need to become authorised as stock exchanges or regulated trading venues) or custodial or wallet providers (as they will need to become authorised for safekeeping and administration), amongst others. Even if a security token does not classify as a transferable security (in particular because that token/coin is not transferable or its transfer is restricted), but provides access to capital or returns for a risk-sharing group of investors, it may classify as a “Capital Markets Act (“CMA”) investment” and its offering may trigger prospectus requirements under the EU Prospectus Regulation unless a prospectus exemption applies.
- Utility tokens: There are many designs of utility tokens. While these are often comparable to vouchers, utility tokens occur in many different forms and also fulfil the function of payment tokens or security tokens (hybrid design), making their classification for supervisory law purposes rather difficult. If the token can only be used for designing a product or a service and is not otherwise associated with any claims, or if the token only grants access to a product or a service without simultaneously serving a payment purpose, then such token will not be covered by supervisory laws. If, on the other hand, the token may be redeemed at the issuer or other users of the platform for the use of a product or a service, then it rather fulfils a payment function similar to a payment token.
- Payment/currency tokens: Tokens that are accepted as means of payment for the purchase of goods or services, or tokens that serve the purpose of transferring money and value but do not confer any claims against a specific issuer (e.g. Bitcoin or Ripple).

Accordingly, due to their specific content/features, security/investment tokens will typically be subject to prospectus requirements (unless an exemption applies), while other types of tokens, such as utility tokens or payment/currency tokens usually will not. No prospectus will need to be published if a prospectus exemption applies. This will be the case if the respective tokens are only offered to qualified investors, or if the offering is directed to fewer than 150 persons who are not qualified investors per EEA Member State, or if the minimum investment is at least €100,000 per investor.

Besides issuers, platform operators may also have the obligation to publish a prospectus, as they may be considered “offerors” for these instruments under the EU Prospectus Regulation. Breaches of the obligation to publish a prospectus are subject to severe sanctions, including under criminal laws.

Taxation

Income tax treatment of cryptocurrencies

In general, capital gains from the sale of cryptocurrencies held as business assets, and income from commercial activities related to cryptocurrencies (e.g. mining, brokerage), are subject to progressive income tax rates of up to 55% for individuals and 25% for corporations.

Special rules apply to cryptocurrencies treated as investment assets and other (non-business) assets:

Cryptocurrencies are treated as investment assets in case the taxpayer uses them to generate interest income. In this case, capital gains from a subsequent sale are taxed at 27.5% for individuals (taxation at lower progressive income tax rates optional) or at 25% for corporations.

In case cryptocurrencies are not used to generate interest income, are only acquired and sold occasionally (private sales) and are not part of a business (non-business assets), capital gains are subject to taxation of up to 55% for individuals only if they are acquired and sold within 12 months. A tax exemption applies if capital gains do not exceed €440 per calendar year. In case cryptocurrencies are held for longer than 12 months, capital gains are not taxable.

VAT treatment of cryptocurrencies

The exchange of cryptocurrencies (e.g. Bitcoin) into fiat currency (e.g. euro) and *vice versa* is VAT-exempt (CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759). Bitcoin mining as such is not subject to VAT because the recipient of the mining services cannot be determined (CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759).

Purchases/supplies of goods or services that are subject to VAT, and which are paid for in cryptocurrency, are treated no differently from payments with fiat currency. The assessment basis for transactions subject to VAT is the fair market value of the units.

Money transmission laws and anti-money laundering requirements

As stated above, money transmission laws may apply to certain business activities involving cryptocurrencies. Cryptocurrencies and tokens used as means of payment may trigger a licensing requirement if they are intended for payment at third parties, and the network within which they can be used to purchase goods/services is large in terms of geographical reach, type of products/services and/or number of accepting parties. Also, if accounts are operated in connection with currencies, payment instruments or means of payment, through which payments are made, the entity holding the accounts may be obliged to become licensed as a payment service provider.

Activities involving cryptocurrencies are subject to anti-money laundering (“AML”) requirements (including know-your-customer (“KYC”) checks and AML prevention systems) if:

- they require a licence under financial services regulation (e.g. as provision of payment services);
- they are subject to AML requirements under commercial law. Pursuant to the Austrian Trade Code (*Gewerbeordnung*; “GewO”), commercial operators, including auctioneers, are subject to AML requirements if they make or receive cash payments of at least €10,000; or
- they relate to providing custodian wallet services (i.e. entities providing services to safeguard private cryptographic keys to hold, store and transfer virtual currencies on behalf of their customers are subject to AML requirements) as providing exchange services between virtual currencies and fiat currencies.

Promotion and testing

True to the government's motto "advice instead of punishment", the Austrian Ministry of Finance has finally implemented a dedicated regulatory sandbox programme that will go live in Fall 2020. In such a sandbox, companies that require a financial services licence will be able to swiftly and comprehensively clarify regulatory requirements for innovative business models in a constant dialogue with the regulator and, if necessary, test such business model based on a scaled-down licence. The selection criteria for admission to the sandbox and further details are based on international best practice.

Ownership and licensing requirements

Cryptocurrencies are currently treated by the Austrian regulator as commodities for supervisory law purposes (see "Cryptocurrency regulation", above). Applicable law as well as internal investment policies may restrict investment managers of certain investors to own cryptocurrencies for investment purposes. For example, Undertakings for the Collective Investment in Transferable Securities ("UCITS") funds, real estate investment funds pursuant to the Austrian Real Estate Investment Funds Act, or staff provision funds and their managers, may not invest in commodities. Pension funds and insurance companies are subject to qualitative and quantitative investment restrictions which will typically not permit direct investment into cryptocurrencies. Depending on the relevant investment policy, AIFs and their managers may, however, invest in cryptocurrencies.

There are currently no specific licensing requirements imposed on an investment advisor or fund manager holding cryptocurrency, over and above those set out under the general trade law/financial services licensing framework.

Mining

Mining Bitcoin and other cryptocurrencies as such is not yet regulated and is thus currently permitted. However, raising capital from the public in order to invest proceeds into mining of cryptocurrencies may be regulated (see "Cryptocurrency regulation" and "Sales regulation", above).

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings.

Reporting requirements

There are currently no reporting requirements for cryptocurrency payments made in excess of a certain value under Austrian law.

Estate planning and testamentary succession

There are no specific rules as to how cryptocurrencies are treated for purposes of estate planning and testamentary succession. Accordingly, general civil law rules apply. Cryptocurrencies qualify as (intangible) assets (*unkörperliche Sache*) for civil law purposes and as such can be included in estate planning/testamentary succession, or form part of a deceased person's estate.

**Ursula Rath****Tel: +43 1 534 37 50412 / Email: u.rath@schoenherr.eu**

Ursula Rath is a partner at Schoenherr in its Vienna office, where she specialises in financial services regulation, capital markets, financings and M&A transactions involving the financial services sector. For over a decade, she has advised issuers, selling shareholders, financial institutions and investors on a wide range of equity and debt capital markets transactions, disclosure requirements, inbound and outbound financial services, conduct of business requirements and compliance. She covers the full range of asset management and investment fund work and has advised clients on regulatory changes, such as under PSD II or MiFID II or on Brexit contingency planning. Ursula is a member of the Fintech Board of the Austrian Ministry of Finance, where she consults on priority actions around start-up financing, ICOs and digital assets and is a founding member of blockchain think tank “thinkBLOCKtank”, a Luxembourg-based, non-profit organisation, bringing together some of the most respected blockchain and distributed ledger experts from currently more than 15 countries (<http://thinkblocktank.org/>). She regularly publishes on financial services regulation, capital markets and funds.

**Thomas Kulnigg****Tel: +43 1 534 37 50757 / Email: t.kulnigg@schoenherr.eu**

Thomas Kulnigg is a partner at Schoenherr, where he specialises in venture capital transactions and start-ups as well as technology transactions. Thomas also leads Schoenherr’s technology & digitalisation group (<https://www.schoenherr.eu/technology-digitalisation/>) and heads the firm’s venture capital and start-up practice.

He is a founding member of think tank “thinkBLOCKtank”, a Luxembourg-based, non-profit organisation, bringing together some of the most respected blockchain and distributed ledger experts from currently more than 15 countries (<http://thinkblocktank.org/>) and is a member of the advisory board of the Digital Asset Association Austria (<https://daaa.at/>).

Schönherr Rechtsanwälte GmbH

Schottenring 19, 1010 Vienna, Austria

Tel: +43 1 534 37 0 / Fax: +43 1 534 37 66100 / URL: www.schoenherr.eu

Canada

Simon Grant, Kwang Lim & Matthew Peters
Bennett Jones LLP

Government attitude and definition

The Canadian federal government is experimenting with blockchain technology throughout different departments. The National Research Council is testing blockchain to publish research grant and funding information in real time.¹ The Canada Border Services Agency is participating in a pilot project designed to improve data quality and facilitate the movement of goods with blockchain-based technology.²

The Bank of Canada is actively conducting research to assess the effects of introducing a central bank digital currency. Senior officials have stated that two main circumstances may warrant the launch of a central bank digital currency: where the use of physical cash is reduced or eliminated; or where private currencies make serious inroads.³ Of these private currencies, officials have suggested that “stablecoins” – crypto assets backed, either fully or in part, by currency or commodity holdings – may be the most promising.⁴ The Bank of Canada has stated that compared to earlier forms of cryptocurrencies, “stablecoins have better prospects for widespread adoption and greater potential to further transform the world of money and payments”.⁵ The Bank of Canada references the Facebook-linked “Libra Coin” as a “strong example of a transformative technology that affects how the Bank needs to respond to the future of money”.⁶

The Bank of Canada has also been involved with “Project Jasper”, a research initiative with Payments Canada and TMX Group that was formed to experiment with the use of distributed ledger technology in the context of payments.

Cryptocurrencies are not treated as legal tender in Canada. According to section 8 of the *Currency Act*, legal tender is coins issued by the Royal Canadian Mint under the *Royal Canadian Mint Act*, and notes issued by the Bank of Canada under the *Bank of Canada Act*.

Cryptocurrency regulation

In Canada, cryptocurrencies are primarily regulated under securities laws as part of the securities’ regulators mandate to protect the public.

Sales regulation

In Canada, securities laws are enacted on a provincial and territorial basis rather than federally. The securities rules throughout the provinces and territories have largely been harmonised. The Canadian Securities Administrators (the “CSA”), an unofficial organisation, represents all provincially and territorially mandated securities regulators in Canada.

Defining a “security”

The securities laws of a province or territory apply to people and entities: (a) distributing securities in that jurisdiction; or (b) from that jurisdiction. “Security” is broadly defined in Canadian securities legislation and covers various categories of transactions, including “an investment contract”. The test for determining whether a transaction constitutes an investment contract, and therefore a security, for the purposes of Canadian securities laws was established by the Supreme Court of Canada, referring to United States jurisprudence. This test, the “**Investment Contract Test**”, requires that in order for an instrument to be classified as a security, each of the following four elements must be satisfied:

1. there must be an investment of money;
2. with an intention or expectation of profit;
3. in a common enterprise (being an enterprise “in which the fortunes of the investor are interwoven with and dependent upon the efforts and success of those seeking the investment, or of third parties”); and
4. the success or failure of which is significantly affected by the efforts of those other than the investor.

The application of the Investment Contract Test has been the subject of judicial and regulatory consideration that is beyond the scope of this overview. That being said, where the elements of the Investment Contract Test are not strictly satisfied, securities regulators in Canada are mandated to consider the policy objectives and the purpose of the securities legislation (namely, the protection of the investing public by requiring full and fair disclosure) in making a final determination. This acts a little like a legislative “basket clause”. The Supreme Court of Canada has stated that substance, not form, is the governing factor in determining whether a contract (or group of transactions) is an investment contract.

Regulator guidance

In addition to the law in Canada as set out in the Investment Contract Test, certain securities regulators in Canada have issued notices and statements regarding the potential application of securities laws to cryptocurrency offerings (“**ICOs**”). These notices and statements confirm that Canadian securities regulators, while receptive to innovation and development, continue to carefully monitor investment activity in this space.

In March 2017, the Ontario Securities Commission (“**OSC**”) issued a press release warning that ICOs may trigger certain Ontario securities law requirements (including registration or prospectus requirements), even if the coins or tokens do not represent shares or equity in an entity.

In August 2017, the CSA issued Staff Notice 46-307 *Cryptocurrency Offerings* (“**SN 46-307**”). In SN 46-307, the CSA stated that it was aware of businesses marketing their coins or tokens as software products, and taking the position that the offerings are exempt from securities laws, but cautioned that “in many cases, when the totality of the offering or arrangement is considered, the coins/tokens should properly be considered securities”, including because they are investment contracts. In line with Canadian jurisprudence and the Investment Contract Test, the CSA affirmed that it will consider substance over form in assessing whether or not securities laws apply to an ICO.

The CSA further cautioned that, depending on the facts and circumstances, coins or tokens may be considered derivatives and subject to applicable legislative and regulatory requirements.

In June 2018, the CSA issued Staff Notice 46-308 *Securities Law Implications for Offerings of Tokens* (“**SN 46-308**”). In SN 46-308, the CSA generally reiterated the position it took

in SN 46-307. Importantly, it again confirmed that an ICO may involve a distribution of securities not covered by the non-exclusive list of enumerated categories of securities in the *Securities Act* (Ontario) if the offering otherwise falls within the policy objectives and purpose of securities legislation. In addition, the CSA indicated that it had found that most offerings of tokens purporting to be utility tokens involved the distribution of a security, and specifically an investment contract.

In March 2019, the CSA and Investment Industry Regulatory Organization of Canada (“**IIROC**”) issued joint Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms* (“**CP 21-402**”). The purpose of CP 21-402 was to seek feedback to establish tailored regulatory requirements for platforms that facilitate the buying and selling or transferring of crypto assets (“**Platforms**”) to address the novel features and risks of Platforms that were not addressed by the existing regulatory framework. CP 21-402 confirmed the guidance set forth in SN 46-307 and SN 46-308, and states that a Platform on which crypto assets that are securities and/or derivatives are traded would be subject to securities and/or derivatives regulatory requirements. It further clarified that if an investor’s contractual right to a crypto asset that is classified as a commodity constitutes a security or derivative, securities legislation could still apply to the Platform on which the crypto asset is traded. Examples of heightened areas of risk compared to other regulated entities, such as marketplaces, are outlined by the CSA and IIROC, and include an investor’s crypto assets not being adequately safeguarded, a lack of transparency of order and trade information, and the potential for manipulative and deceptive trading.

CP 21-402 outlines a Proposed Platform Framework (the “**PPF**”) that will apply to Platforms that operate in Canada and Platforms with Canadian participants, and is based on the regulatory framework for marketplaces. The PPF incorporates requirements relevant for dealers and is structured to account for the different marketplace and dealer functions that Platforms may perform. Furthermore, the PPF also considers Platforms becoming IIROC dealer and marketplace members and becoming registered as investment dealers.

In January 2020, the CSA issued Staff Notice 21-327 *Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets* (“**SN 21-327**”).⁷ This notice provides clarity on what types of Platforms trigger securities regulation. SN 21-327 addresses the flexible nature of crypto assets and further adopts the substance-over-form test in determining whether a crypto asset that trades on a Platform is considered a security. Generally speaking, this determination hinges on the rights associated with the assets traded, as well as the timeline for settlement for each given transaction.

If a Platform trades in crypto assets that attach certain properties such as voting rights or rights to receive dividends, those assets will likely trigger securities regulation as they are already clearly defined as securities.⁸ Additionally, if a Platform retains a purchaser’s crypto assets internally, such as through a virtual wallet, instead of making immediate delivery of an asset, those assets will likely be treated as securities by the CSA.⁹ SN 21-327 also notes the importance of examining the typical commercial practice in determining whether a crypto asset is a security. For instance, some Platforms may state in their agreement that assets are to be immediately delivered, but it may instead be common practice that the Platforms retain those assets in a wallet instead. Where a Platform, through whatever means, retains ownership, control and possession of the crypto assets traded, securities regulations will likely apply. In these instances, users are reliant on the Platform and become exposed to ongoing credit, fraud, performance, and proficiency risk on the part of the Platform.¹⁰

Generally, the CSA recommends that Platforms consult legal counsel on the application of securities legislation and contact their local securities regulatory authority to discuss whether securities legislation applies to their activities and, if so, the appropriate steps to achieve compliance.¹¹

In October 2019, a panel of the OSC permitted a fund managed by 3iQ Corp. (“**3iQ**”) to become the first publicly traded Bitcoin investment fund in Canada.¹² In making its decision, the OSC took into consideration that Bitcoin is an asset with sufficient liquidity to satisfy Canadian securities regulation, in part due to the fact that a variety of trading platforms are available to help facilitate the sale of Bitcoin and properly value price. This decision appears to be a step towards more widespread adoption of crypto assets in traditional financial markets.

Securities law requirements

In Canada, absent an available exemption, a prospectus must be filed and approved with the relevant regulator before a person or entity can legally distribute securities. A prospectus is a comprehensive disclosure document which seeks to satisfy the public protection aim of securities laws by disclosing information about the securities and the issuer to prospective investors. Exemptions from the prospectus requirement are principally set out in National Instrument 45-106 *Prospectus Exemptions* (“**NI 45-106**”). Generally, securities sold pursuant to a prospectus exemption are subject to resale restrictions and, particularly in the case of a non-reporting issuer (*i.e.*, an issuer that is not a public entity and is not subject to ongoing securities compliance and disclosure obligations), may never be freely tradeable. Resale restrictions rules are set out in National Instrument 45-102 *Resale of Securities* (“**NI 45-102**”).

In addition to the prospectus requirement, an individual or entity engaged in the business of distribution of securities, or advising others with respect to securities, is required to register with Canadian securities regulators. The requirements for registration, and exemptions from registration, are set out in National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (“**NI 31-103**”). Once registered, the person or entity is subject to various reporting and compliance obligations. NI 31-103 covers various other categories of registration in addition to dealers and advisers, such as investment fund managers.

Legal status of ICOs in Canada

The present Canadian regulatory trend is to apply and adapt existing securities laws, including the Investment Contract Test, to transactions involving blockchain or cryptocurrency that resemble traditional securities, without regard to the use of new technology. In order to make a determination on whether or not an ICO constitutes a distribution of securities, Canadian securities regulators will perform a case-by-case, highly fact-dependent analysis, focusing on the substance and structure of the ICO rather than its form. Even if an ICO cannot be said to fall within the specific definition of a “security” provided by legislation, as discussed above, it may nonetheless be found to involve the sale of securities if it otherwise triggers the policy objectives and purposes of securities legislation.

Applying the Investment Contract Test to ICOs

Statements from the CSA offer guidance regarding certain elements of an ICO that may increase the likelihood of the coins or tokens being found to be securities. While each offering of coins or tokens should be analysed based on the particular circumstances of the

offering and the features of the coin or token, these statements, together with statements by United States securities regulators on the subject, offer insight into how the Investment Contract Test may be applied to ICOs.

Coins or tokens as securities

If an ICO is found to constitute a distribution of securities, it will trigger Canadian securities law requirements, including prospectus and registration requirements, unless an exemption from the same is available. Individuals or businesses intending to rely on prospectus exemptions in connection with an ICO will need to ensure that they satisfy the conditions for such exemption as set out in NI 45-106, including any applicable resale restrictions in NI 45-102. Resale restrictions will be of particular concern if coins or tokens begin trading on cryptocurrency exchanges or otherwise in the secondary market following their initial sale. Issuers of a cryptocurrency that is found to be a security will also need to ensure that they comply with any applicable registration requirements, including dealer registration, or that the conditions for an exemption from registration are fully satisfied. Failure to comply with securities laws may result in regulatory or enforcement action by securities regulators against the parties behind the ICO, including fines and potential incarceration.

Taxation

Background

The Canadian tax treatment of cryptocurrencies remains uncertain, with little legislative authority or administrative guidance. The Canadian federal tax authority (the Canada Revenue Agency, or “CRA”) has expressed high-level views regarding the characterisation of certain payment tokens (*i.e.*, Bitcoin) and the potential income and sales tax implications of crypto mining and certain commercial transactions using tokens; however, these views are extremely limited.¹³ Moreover, while the Canadian federal government has been making strides to address the void and clarify certain ambiguities, much work remains to be done in order to solidify the underlying tax regime.

Much of the analysis thus far concerning the potential tax treatment in Canada of cryptocurrency transactions is founded in an extrapolation of these administrative positions and thin legislative framework to scenarios upon which Canadian legislators and tax administrators have not expressly considered. It is hoped that greater clarity will be provided in the near future that will not be limited to Bitcoin/payment instruments, but will also consider more recent developments in cryptocurrency technologies and their evolving distribution to, and usage by, the public, including ICOs.¹⁴

Characterisation of cryptocurrency for income tax purposes

The CRA currently adopts the position that, despite its nomenclature, a cryptocurrency (specifically, a payment token such as Bitcoin) is not a “currency” for income tax purposes. Rather, such a cryptocurrency is akin to a commodity (albeit an “intangible”), the value of which will fluctuate based on external factors driven largely by investor sentiment and basic supply/demand. Based on this view, this type of cryptocurrency could potentially be analogised as the virtual equivalent of a precious metal such as gold or silver. Such a characterisation, if appropriate, could have significantly different tax implications under Canadian tax law as compared to “normal” cash (even foreign currency) transactions. Note that the CRA has generally been silent on its views concerning cryptocurrencies other than payment tokens (*i.e.*, Bitcoin). Accordingly, references below to “cryptocurrency” are generally restricted to payment tokens unless otherwise indicated.

(a) *Acquisition of cryptocurrency*

The threshold question is whether the initial acquisition of a cryptocurrency is a taxable event that potentially triggers a Canadian income tax liability to the person acquiring the cryptocurrency. The answer depends on the manner, purpose and circumstances in which the cryptocurrency is acquired.

The acquisition of cryptocurrency as a pure speculative investment, similar to physical gold or a publicly traded security, is generally not a taxable event to the person acquiring the cryptocurrency. However, the acquisition will establish the holder's "cost" in the cryptocurrency for Canadian tax purposes, which is relevant in the determination of the tax consequences that will be realised later when the cryptocurrency is eventually sold or otherwise exchanged.

This is to be contrasted with the acquisition of cryptocurrency as consideration for the provision of goods or services, or as compensation for some other right of payment. Such transactions are generally governed at this time by the CRA's position regarding "barter transactions", which is described in greater detail below under the heading "*Using cryptocurrencies in business transactions – Barter transaction*".

Where cryptocurrency has been acquired as a result of "mining" activities of a commercial nature, the current administrative position of the CRA suggests that the miner is subject to income tax at the time the cryptocurrency is earned. This is based on the concept that the mining activities are a service and that the mined cryptocurrency is received as compensation for those services. As with other services that are compensated with cryptocurrency, the CRA applies its position regarding barter transactions in determining the amount that is required to be included in income at the time the cryptocurrency is earned. This is an evolution of prior CRA administrative guidance regarding crypto mining, providing greater clarity regarding the quantum and timing of income recognition for miners.

(b) *Determining a holder's tax cost in cryptocurrency*

Once a cryptocurrency has been acquired, it will be important to determine its cost for Canadian tax purposes, which is a fundamental concept for determining the future income tax consequences on an eventual disposition of the cryptocurrency.

Where a cryptocurrency is purchased in exchange for Canadian currency, the cost of the cryptocurrency for income tax purposes will be equal to the amount of cash paid, plus any directly related acquisition expenses. If foreign currency is used, the holder will generally be required to convert the foreign currency into the Canadian-dollar equivalent at the applicable rate, pursuant to Canadian tax rules.

Cryptocurrencies can obviously be acquired by several alternative means, including commercial business transactions and other forms of "barter" exchanges. The particular facts surrounding any such acquisition could have meaningful distinctions regarding the determination of the holder's tax cost upon the acquisition of the cryptocurrency (see below, under the heading "*Using cryptocurrencies in business transactions – Barter transaction*").

(c) *Tax on disposition of cryptocurrency*

A person will realise taxable income (or loss) on an eventual disposition of a cryptocurrency. This includes a sale of the cryptocurrency for cash and the use of the cryptocurrency to pay for goods or services, or as consideration under other contractual rights/obligations (*i.e.*, a "barter transaction", described below).

If the cryptocurrency has a value at the time of its disposition in excess of its tax cost, it will be critical to determine whether the holder should report such excess as being on capital

account (*i.e.*, a capital gain) or whether the proceeds should be reported as business income. This is a material distinction for tax purposes.

Generally, the buying and selling of cryptocurrencies can be regarded as being on capital account unless it is carried out in the context of a business of buying and selling such cryptocurrencies, or such buying and selling otherwise amounts to an “adventure or concern in the nature of trade”. This is a factual, case-by-case determination requiring a detailed review of the holder’s dealings with cryptocurrencies.

If a person acquires cryptocurrency as payment for goods or services in the normal course of the person’s business (even if the person is not, *per se*, in the business of buying and selling cryptocurrencies as part of a speculative investment business), there is a risk that any appreciation realised when the person disposes of the cryptocurrency will be fully taxable as business income. Again, this issue is fact-dependent, should be reviewed on a case-by-case basis, and is described in greater detail below.

Using cryptocurrencies in business transactions

(a) Barter transaction

A person can accept a commodity in exchange for the provision of a good or service or as consideration for some other form of right of payment, with such transaction being subject to tax treatment under Canada’s “barter transaction” tax rules.

In a barter transaction using cryptocurrency, the following must be considered by the person (referred to below as the “provider”) that accepts a cryptocurrency as consideration in exchange for a good, service or other right:

- The provider will generally realise business income for Canadian income tax purposes equal to the fair market value of the goods, services or other rights provided (the “**Business Income Inclusion**”). For this purpose (but not for other purposes – see, *e.g.*, the sales tax implications described below), the value of the cryptocurrency at the time of the exchange is generally not the determining factor.
- The provider will generally acquire the cryptocurrency with a cost for Canadian income tax purposes equal to the Business Income Inclusion.
- The provider is now the owner of the cryptocurrency and must (eventually) do something with it, such as sell it to an investor or use it to purchase goods/services/rights in connection with its own business. Any gain or loss realised by the provider on an eventual disposition of the cryptocurrency (*i.e.*, the difference between the provider’s cost in the cryptocurrency, and the amount received on the eventual disposition) will be taxable at such time to the provider. The issue then becomes whether such gain/loss is treated as being on full income account or on account of capital (the income tax treatment being materially different as between the two) (see the discussion above under the heading “*Characterisation of cryptocurrency for income tax purposes – Determining a holder’s tax cost in cryptocurrency*”). Managing the provider’s exposure to fluctuations in the value of the cryptocurrency post-acquisition will be a material and practical concern.

Another type of increasingly prevalent transaction (which may or may not be properly characterised as a “business transaction”) is the acquisition by a person of one cryptocurrency (“crypto #1”) in exchange for a different cryptocurrency (“crypto #2”). Such a transaction will also be considered a barter transaction involving the exchange of one commodity for another commodity. The person will generally be considered to have acquired crypto #1 with a tax cost equal to the fair market value of the crypto #2 given up in exchange, computed as of the time of the barter transaction. The additional complication in this scenario is that the

person acquiring crypto #1 will also be considered to have disposed of crypto #2, and will have to report any income/gain in respect of crypto #2 for Canadian income tax purposes (the person must therefore know his/her tax cost in crypto #2, which depends on the manner in which crypto #2 was originally acquired by such person).

(b) Sales tax implications

Canada imposes a federal sales tax (the goods and services tax, or “GST”) on the supply of many goods and services, subject to detailed exemptions. Most Canadian provinces and territories also levy sales tax, which is often “harmonised” with the federal sales tax to effectively create one blended federal/provincial (or territorial) rate. Persons who are required to charge and collect federal GST (or harmonised sales tax) in respect of a business activity can generally claim a rebate in respect of such tax that the person directly incurs in the course of carrying on such business (generally referred to as an input tax credit, or “ITC”). The ITC mechanism is generally intended to mitigate the duplication of sales tax throughout a supply chain, and is designed to ensure that the cost of sales tax is ultimately borne solely by the end consumer of any particular good or service.

As with any provision of goods or services subject to federal and provincial/territorial sales taxes, a provider of goods/services that accepts cryptocurrency *in lieu* of government-issued currency must charge, collect and remit the appropriate sales tax. This may prove easier said than done in the context of cryptocurrency.

In this respect, the provider must be careful not to use the Business Income Inclusion amount (which is relevant under the Canadian tax authorities’ current administrative policy to determine the provider’s income tax associated with the sale) in determining the applicable amount of sales tax. For federal GST purposes, the Canadian tax authorities require that the provider charge, collect and remit GST based on the value of the cryptocurrency at the time of the sale. Presumably, the purchaser would be entitled to claim an ITC (if available) in respect of the full GST charged, if incurred in the course of a business activity.

While this may sound manageable at a high level, a few practical issues arise for the provider:

- How does the provider determine the value of the cryptocurrency at the precise moment of sale, particularly when cryptocurrencies are traded in non-traditional marketplaces and the value can swing wildly from day to day (possibly minute by minute)? What record-keeping is required by the service provider to justify the amount upon which it charges sales tax?
- How does the provider charge, collect and remit the sales tax in a transaction entirely handled in cryptocurrency, namely where the sales tax portion is also paid in cryptocurrency? The provider must remit to the Canadian tax authorities in Canadian currency (not cryptocurrency), meaning that the provider will be forced to either remit an equivalent amount of cash from other sources, or sell a sufficient amount of the cryptocurrency to generate the cash to satisfy the remittance. Given the volatility of most cryptocurrencies, an inherent risk is borne by the provider in collecting the sales tax in cryptocurrency.

Corporate directors are personally liable for any deficiencies in collecting or remitting sales tax. It is therefore critical for the provider of goods/services to take reasonable measures to ensure full compliance and mitigate any associated risk.

Another sales tax issue associated with transactions involving cryptocurrencies is whether the person disposing of the cryptocurrency (*e.g.*, the person using the cryptocurrency to purchase goods or services or trading one cryptocurrency for another) is required to charge

and collect sales tax on the value of the cryptocurrency. In this respect, if the disposition of a cryptocurrency is a barter transaction akin to a disposition of a commodity, should such disposition be treated as a taxable supply of the cryptocurrency much in the same way as a commodity? If that were the case, compliance obligations and costs associated with routine cryptocurrency transactions could become exceedingly complex and beyond the reasonable abilities of many holders/users of cryptocurrency. In May 2019, the Canadian Department of Finance released draft legislation aimed at simplifying the federal sales tax on certain transactions involving “virtual payment instruments” (“VPIs”). In this respect, a VPI generally includes payment tokens such as Bitcoin, but expressly excludes tokens that operate in a manner similar to gift cards or that have functionality on a gaming or affinity/rewards programme platform. Pursuant to these proposals, transactions involving VPIs would generally be exempt from federal sales tax as a “financial instrument”. These proposals, which have yet to be passed into law, demonstrate a willingness of the Canadian federal government to tackle the difficult tax and compliance issues associated with cryptocurrencies, albeit in only a fairly narrow and targeted manner at this time.

Money transmission laws and anti-money laundering requirements

Canada was the first country to approve regulation of cryptocurrencies in the context of anti-money laundering (“AML”). In 2014, a bill was passed to amend the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (“PCMLTFA”) to include virtual currencies through a framework for regulating entities “dealing in virtual currencies”, treating them as money services businesses (“MSBs”). As MSBs, those dealing in digital currencies are subject to the same record-keeping, verification procedures, suspicious transaction reporting and registration requirements as MSBs dealing in fiat currencies.¹⁵

The PCMLTFA was amended in June 2019¹⁶ to expand the definition of virtual currencies to include tokens that can be used either for payment purposes (such as Bitcoin or stablecoin) or for investment purposes (such as security tokens). It also required dealers that qualify as MSBs to register with the Financial Transactions and Reports Analysis Centre of Canada (“FINTRAC”) and implement a complete AML compliance plan that is independently assessed.

In February 2020, the Virtual Currency Travel Rule, which requires financial entities and MSBs to keep a record of electronic funds transfers executed cross-border,¹⁷ was expanded to require financial entities and MSBs to include virtual currency transactions as well, meaning crypto asset dealers that participate in cross-border transactions are subject to enhanced due diligence measures set out by the Act.

Although the requirement that MSBs register with FINTRAC and implement complete AML compliance plans will not take effect until June 2021, the cross-border reporting and identification requirements set out by the PCMLTFA in February have been in effect since June 2020.

Promotion and testing

The CSA Regulatory Sandbox was set up to encourage the development of innovative products and services. The Sandbox allows companies engaged in cryptocurrency matters to register or seek exemptive relief (generally on a time-limited basis) in order to test products and services in the Canadian market. SN 21-327 also expands the application of the CSA Regulatory Sandbox to relevant crypto asset trading platforms.¹⁸

Ownership and licensing requirements

As noted above, an individual or entity engaged in the business of distribution of securities, or advising others with respect to securities, may be required to register with Canadian securities regulators. Similarly, investment fund managers are required to be registered.

On December 11, 2017, IIROC, the organisation that governs persons and companies registered under securities law, issued a notice to its members regarding margin requirements for cryptocurrency futures contracts that trade on commodity futures exchanges. According to the notice, members are required to market and margin crypto futures contracts daily at the greatest of: (a) 50% of market value of the contracts; (b) the margin required by the futures exchange on which the contracts are entered into; (c) the margin required by the futures exchange's clearing corporation; and (d) the margin required by the Dealer Member's clearing broker.

Mining

Because mining converts electrical energy (typically drawn from the power grid or a private power source) into waste heat in proportion to the difficulty of the underlying mathematical problem, it can result in large quantities of power being used for what may be perceived as a socially undesirable purpose. Furthermore, because mining enables the operation of a variety of cryptocurrencies (e.g., Bitcoin), it functions as a convenient point for regulatory intervention. For those reasons, many official bodies have started to explore, or in some cases have implemented, laws or policies that contemplate cryptocurrency mining. In Canada, governmental regulators appear to have adopted a largely "hands-off" approach for the time being.

However, Hydro-Québec (a Québec Crown entity) recently announced the implementation of restrictions on energy allocation to 300 megawatts for users involved in cryptocurrency mining, the effect of which may be to discourage such activities in that province. We expect to see further intervention by government actors, as the quantity of power used by cryptocurrency mining operations, along with the use of various cryptocurrencies to facilitate illegal activities, continues to grow. To counteract the deleterious effects of such regulations on their operations, we additionally expect to see Bitcoin miners move to private power sources as time goes on.

Border restrictions and declaration

There are no border restrictions or declaration requirements as such.

However, as discussed above, dealers in crypto assets that qualify as MSBs are now subject to the record-keeping requirements of the Virtual Currency Travel Rule under the PCMLTFA, which requires these dealers to keep a record of the transfer with the personal information of both parties to the transaction, as well as being required to take reasonable measures to ensure that any transfer received includes such information.

Reporting requirements

See "*Money transmission laws and anti-money laundering requirements*", above. MSBs are required to send a large cash transaction report to FINTRAC upon receipt of an amount of \$10,000 or more in cash in the course of a single transaction, or upon receipt of two or more cash amounts of less than \$10,000 each that total \$10,000 or more if the transactions were made by the same individual or entity within 24 hours of each other.

Estate planning and testamentary succession

Canada levies no separate estate tax, unlike many countries. However, a deceased is deemed to dispose of their property on death for its fair market value, which can result in income taxes being payable by the estate. Although it is far from settled, the CRA currently takes the view that cryptocurrencies are generally commodities rather than currency, and that trading in cryptocurrencies will usually (with some possible exceptions) be regarded as being on capital account. In such circumstances, the estate will have to pay tax on any capital gains accrued as of the date of death. For a more detailed discussion of tax issues, see “*Taxation*”, above.

In terms of estate planning, given the anonymous, decentralised nature of cryptocurrencies held on a blockchain, it will be imperative to include instructions on where to locate a copy of the private key related to the cryptocurrency. It would be unwise to include a private key in the will itself, since wills generally become public documents following probate.

* * *

Endnotes

1. <https://globalnews.ca/news/3977745/ethereum-blockchain-canada-nrc/>.
2. <http://nexus.gc.ca/new-neuf/articles/blockchain-chaine-blocs-eng.html>.
3. Bank of Canada, *Money and Payments in the Digital Age*, Remarks by Timothy Lane, Deputy Governor, CFA Montreal Fintech RDV2020, February 2020.
4. *Ibid.*
5. *Ibid.*
6. *Ibid.*
7. See Canadian Securities Administrators, Staff Notice 21-327 – Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets at <https://www.osc.gov.on.ca/en/61530.htm>.
8. *Ibid.*
9. *Ibid.*
10. *Ibid.*
11. See Canadian Securities Administrators, Staff Notice 21-327 – Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets at <https://www.osc.gov.on.ca/en/61530.htm>.
12. 3iQ Corp (Re), 2019 ONSEC 37.
13. Certain provincial tax authorities, namely Revenu Québec, have also published their own administrative positions on certain narrow issues (*i.e.*, provincial sales tax) dealing with cryptocurrencies.
14. The taxation of ICOs is beyond the scope of this chapter, due to: (i) the significant differences in potential ICO structures and legal characterisation of the underlying transactions; (ii) the speed at which ICO structure and cryptocurrency “technology” and forms of offerings are evolving; and (iii) the lack of meaningful legislative, judicial or administrative guidance from a Canadian tax perspective. However, the fundamental “building block” tax concepts discussed in this chapter likely form the basis of the analysis underpinning certain of the discrete transactions and legal relationships created in many current ICO structures.

15. See United States Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, SEC Release No 81207 (July 25, 2017).
16. Regulations Amending Certain Regulations Made Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, 2019: SOR/2019-240, *Canada Gazette*, Part II, Volume 153, Number 14 at page 2.
17. Regulations Amending the Regulations Amending Certain Regulations Made Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, 2019, *Canada Gazette*, Part II, Volume 154, Number 12.
18. *Ibid.* at note 1.

* * *

Acknowledgments

The authors thank Esther Peterson and Benjamin Sissons for their assistance with this chapter.

**Simon Grant****Tel: +1 416 777 6246 / Email: Grants@bennettjones.com**

Simon Grant is a co-head of Bennett Jones' cross-disciplinary Fintech & Blockchain practice group. Simon practises corporate law with an emphasis on financing transactions and financial regulation.

Simon regularly advises clients on financial regulation and compliance, including foreign financial institutions and fintech companies doing business in Canada.

He also routinely acts for credit providers, borrowers and sponsors on loan facilities, acquisition financings, project financings and capital markets transactions.

**Kwang Lim****Tel: +1 604 891 5144 / Email: LimK@bennettjones.com**

Kwang Lim is a member of the Fintech & Blockchain practice group. His business law practice includes corporate finance and M&A. He focuses on offering practical and strategic advice and facilitating opportunities for domestic and international clients, including entrepreneurs, start-ups, scale-ups, public companies, and broker-dealers across various industry sectors. Kwang also advises on securities law compliance and corporate governance issues.

Kwang is an adjunct professor at the Faculty of Law, University of British Columbia where he teaches the Business Law Capstone course.

Kwang obtained his Master of Laws at the University of California, Los Angeles with a specialisation in business law.

**Matthew Peters****Tel: +1 416 777 6151 / Email: PetersM@bennettjones.com**

Matthew Peters advises clients in various industries, including natural resources, manufacturing, financial services, telecommunications, pharmaceuticals and technology, in connection with international tax planning, domestic and cross-border mergers and acquisitions, corporate reorganisations, corporate finance, executive and employee compensation and various other tax matters. He has also represented clients before the Tax Court of Canada and the Federal Court of Appeal.

Matthew is a frequent speaker on international and domestic tax matters, and has written and presented papers at conferences and seminars across Canada and the United States. He is a member of the Canadian and Ontario Bar Associations, Canadian Tax Foundation, New York State Bar Association, American Bar Association and International Fiscal Association.

Bennett Jones LLP

3400 One First Canadian Place, P.O. Box 130, Toronto, ON, M5X 1A4, Canada

Tel: +1 416 777 4801 / Fax: +1 416 863 1716 / URL: www.bennettjones.com

Cayman Islands

Alistair Russell & Jenna Willis
Carey Olsen

Government attitude and definition

The Cayman Islands is a leading global financial centre and has, over the course of several decades, developed a reputation as one of the world's most innovative and business-friendly places to operate. The jurisdiction offers a stable society and political system, judicial and legislative links to the United Kingdom, tax neutrality, sophisticated service providers, and a proportionate regulatory regime that focuses closely on the financial services industry, and in particular those catering to sophisticated and institutional investors based elsewhere.

It is this reputation and these attributes that have helped the jurisdiction become an obvious choice for many of those proposing to establish fintech-related structures, whether it be in the form of a fund vehicle investing into digital assets, an exchange for the same, an initial coin offering, or otherwise.

Each of the Cayman Islands Government, the Cayman Islands Monetary Authority (“**CIMA**”), and industry bodies such as Cayman Finance and the Cayman Islands Blockchain Foundation, acknowledge the importance of continuing to attract fintech business to the jurisdiction and ensuring the further growth of the sector. They are also aware, however, of the need to balance this approach with maintaining the Cayman Islands' commitment to the highest standards of financial probity and transparency and the specific considerations that can accompany digital assets.

Consequently, in May 2020, recognising the newly adopted international standards set by the Financial Action Task Force, a new framework for the supervision and regulation of virtual asset services businesses was introduced in the Cayman Islands, namely the Virtual Asset (Service Providers) Law, 2020 (the “**VASP Law**”). The features of the VASP Law are described further in this chapter; however, it is important to note that at the time of writing, this new legislation is not yet in force and some details of the regulatory regime are in the process of being finalised. A specific date for implementation of the VASP Law is not yet known, but it is expected to be in the near term.

Overall, the new framework continues to make the Cayman Islands an attractive jurisdiction for virtual asset services businesses, as it provides a flexible regulatory foundation while furthering Cayman's commitment to international standards.

Under the VASP Law, a “**virtual asset**” is broadly defined as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Specifically excluded from this are digital representations of fiat currencies, as well as “virtual service tokens”, which are digital representations of value that are *not* transferrable or exchangeable with a third party at any time (including digital tokens whose sole function is to provide access to an application or service or to provide a service or function directly to its owner).

Cryptocurrency regulation

The VASP Law clearly establishes the legitimacy of cryptocurrencies in the Cayman Islands and will regulate businesses providing services related to virtual assets. Virtual assets themselves and parties dealing with virtual assets for their own purposes are generally not subject to specific regulation in the Cayman Islands.

Under the VASP Law (once it is in force), all virtual asset service providers will be required to be licensed or registered with CIMA, obtain a waiver or hold a sandbox licence. A “virtual asset service provider” (a “**VASP**”) is an entity that is incorporated or registered in the Cayman Islands, which provides a virtual asset service as a business or in the course of business.

A “**virtual asset service**” for this purpose means the issuance of virtual assets or the business of providing any of the following services or operations for or on behalf of another person or entity:

- (a) exchange between virtual assets and fiat currencies;
- (b) exchange between one or more other forms of convertible virtual assets;
- (c) transfer of virtual assets;
- (d) virtual asset custody service, which is the business of safekeeping or administration of virtual assets or the instruments that enable the holder to exercise control over virtual assets; or
- (e) participation in, and provision of, financial services related to a virtual asset issuance or the sale of a virtual asset.

Cryptocurrency and other digital asset businesses which are not caught by any of the above categories may still be subject to regulation in the Cayman Islands which does not specifically target digital assets, such as the Securities Investment Business Law, the Money Services Law and anti-money laundering (“**AML**”) regulations (each described further below).

Sales regulation

VASP Law

As set out above, the issuance of virtual assets, the provision of financial services related to a virtual asset issuance or the sale of a virtual asset, as well as the transfer of virtual assets, if being carried out by a Cayman Islands entity as a business on behalf of another party, will likely constitute virtual asset services and require a licence or registration with CIMA under the VASP Law (once in force).

Under the VASP Law, any issuance of virtual assets will require CIMA’s prior approval. For this purpose, an issuance means the sale of newly created virtual assets to the public in exchange for fiat currency, other virtual assets or other consideration. “Public” is not defined in the VASP Law so should be interpreted broadly for this purpose; however, limited private sales may in some cases not be captured. The sale of virtual service tokens will also be excluded from this requirement and any sale that is not for consideration (e.g. a bonus) should be excluded.

Direct issuances will be subject to a prescribed maximum threshold, which, at the time of writing, has not been fixed. The threshold will not apply where the issuance is done by way of one or more virtual asset trading platforms, provided that the relevant platforms are either licensed under the VASP Law or regulated in another non-high-risk jurisdiction.

Investment funds

An entity that operates as an investment fund that is formed or registered in the Cayman Islands and that issues digital assets may come within the ambit of the Mutual Funds Law

(for open-ended funds) or the Private Funds Law (for closed-ended funds), and be required to obtain a registration or licence thereunder to the extent such digital assets constitute equity or investment interests. This will of course depend on a number of aspects, including the terms of the issue and the nature of the assets, and specific advice should be sought. For example, under the Mutual Funds Law, the definition of “equity interest” has recently been amended to include “any other representation of an interest”, which is likely broad enough to capture a variety of forms of digital asset.

Additionally, any pooling vehicle that is investing into the digital asset space, or accepting digital assets by way of subscription and then investing into more traditional asset classes, would be advised to seek Cayman Islands legal advice on the point.

Securities Investment Business Law

Pursuant to the Securities Investment Business Law of the Cayman Islands (“SIBL”), an entity formed or registered in, or that is operating from, the Cayman Islands that engages in dealing, arranging, managing or advising on the acquisition or disposal of digital assets, may come within the ambit of SIBL and be required to obtain a registration or licence from CIMA thereunder (which may be in addition to a registration or licence required under the VASP Law). This applies to the extent that the relevant digital assets constitute “securities” for the purposes of SIBL.

Notably, the definition of “securities” thereunder includes virtual assets which can be sold, traded or exchanged immediately or at any time in the future that (i) represent or can be converted into another form of traditional securities (e.g. equity interests, debt instruments, options or futures), or (ii) represent a derivative of traditional securities. Consequently, consideration will need to be given on a case-by-case basis as to whether the digital asset in question falls within one of the above categories.

Offerings within the Cayman Islands

In relation to the offering, sale, or issuance of interests within the Cayman Islands, certain regulatory provisions should be borne in mind. For example, the Companies Law prohibits any exempted company formed in the Cayman Islands and not listed on the Cayman Islands Stock Exchange from offering its securities to the Cayman Islands public. The Limited Liability Companies Law includes a similar prohibition in relation to limited liability companies (“LLCs”). Even persons based, formed or registered outside the Cayman Islands should be careful not to undertake any activities in relation to a sale or issuance of digital assets that would constitute “carrying on a business” in the Cayman Islands. To do so may entail various registration and licensing requirements and financial and criminal penalties for those who do not comply. There is no explicit definition of what will amount to “carrying on a business” for these purposes and, consequently, persons who propose to undertake concerted marketing to the Cayman Islands public, particularly if it involves engaging in any physical activity in the Cayman Islands, are encouraged to seek specific legal advice.

In practice, however, these restrictions do not generally pose a significant practical concern for issuers given that:

- (i) the “public” in this instance is taken to exclude other exempted companies, exempted limited partnerships, and LLCs (which together comprise the majority of Cayman Islands entities); and
- (ii) issuers’ target investors tend not to include other persons physically based in the Cayman Islands.

Taxation

There are no income, inheritance, gift, capital gains, corporate, withholding or other such taxes imposed by the Cayman Islands Government, including with respect to the issuance, holding, or transfer of digital assets.

Stamp duty may apply to original documents that are executed in the Cayman Islands or are brought into the Cayman Islands following execution. However, the sums levied are generally of a nominal amount.

Entities formed or registered in the Cayman Islands may apply for and, upon the payment of a fee of approximately US\$1,830, receive a tax exemption certificate confirming that no law enacted in the Cayman Islands after the date thereof imposing any tax to be levied on profits, income, gains or appreciations shall apply to such entity or its operations. Such certificates will generally apply for a period of between 20 and 50 years (depending on the type of entity).

Money transmission laws and anti-money laundering requirements

Money transmission laws

Pursuant to the Money Services Law, any person carrying on a “money services business” in or from the Cayman Islands must first obtain a licence from CIMA thereunder. Any breach of this requirement will constitute a criminal offence.

For the purposes of the foregoing, a “money services business” means the business of providing, among other things, money transmission or currency exchange services.

Although there is no clear authority on the extent to which the foregoing would be seen to include such transactions in cryptocurrency or other digital assets, a cautious and substantive reading of the statute may, in some cases, warrant it. In particular, if the digital assets in question are primarily used to facilitate the transfer of fiat currency from one party to another, or the conversion between fiat currencies, the legislation may well apply. Consequently, persons wishing to establish such businesses are encouraged to consider closely the application of the Money Services Law and consult appropriate advisors.

Anti-money laundering requirements

The very nature and, in some cases, the intended features of digital assets can present heightened compliance risks and practical hurdles to addressing the same. Such features may include the lack of a trusted central counterparty, increased anonymity, and ease of cross-border transfer without any gating or restriction.

Consequently, the Cayman Islands authorities have maintained a keen focus on balancing the jurisdiction’s long track record of innovation and the promotion of a business-friendly environment with its commitment to the prevention of crime and maintaining robust standards of transparency. In general, this has been done not by establishing an entirely separate regime for digital assets, but by applying the purposive approach enshrined within the existing framework which focuses on the specific activity and the nature of the assets in question so as to properly quantify the risk that the same may be used to facilitate illegal activity.

Pursuant to the provisions of the Proceeds of Crime Law, the Anti-Money Laundering Regulations, and the guidance notes thereon (together, the “**AML Laws**”), any persons formed, registered or based in the Cayman Islands conducting “relevant financial business” are subject to various obligations aimed at preventing, identifying, and reporting money laundering and terrorist financing.

“Relevant financial business” is defined in the Proceeds of Crime Law and includes the provision of virtual asset services (which is defined slightly differently for this purpose than under the VASP Law). We would thus generally expect cryptocurrency businesses to come within the scope of the AML Laws.

Although a detailed consideration of the specific requirements of the AML Laws falls outside of the scope of this chapter, any person subject to the regime will generally need, among other things, to do the following:

- appoint a named individual as an AML compliance officer to oversee its adherence to the AML Laws and to liaise with the supervisory authorities (and, under the VASP Law, a VASP must have such officer approved by CIMA);
- appoint named individuals as the money laundering reporting officer and a deputy for the same to act as a reporting line within the business; and
- implement procedures to ensure that counterparties are properly identified, risk-based monitoring is carried out (with specific regard to the nature of the counterparties, the geographic region of operation, and any risks specifically associated with new technologies such as virtual assets), proper records are kept, and employees are properly trained.

In addition, CIMA has issued specific AML-related guidance for VASPs and new regulatory requirements have been put in place to ensure sufficient information is obtained relating to transfers of virtual assets by intermediaries.

In our experience, most parties will be best advised to consult specialist third-party providers to assist with this process.

Promotion and testing

Sandbox licences

The VASP Law, once in force, will introduce a sandbox licence, intended for providers of virtual asset services or other fintech services that utilise innovative technology or use an innovative method of delivery. A sandbox licence provides flexibility, such that CIMA can impose additional requirements or allow certain exemptions, to cater for the relevant business.

A sandbox licence will be temporary, available for a maximum of one year, during which we anticipate that CIMA will assess how best to regulate the business in the future, including whether that requires legislative change, to further promote and monitor the use of the relevant innovation.

Special Economic Zone

Additionally, the Cayman Islands Government has been active in promoting the Special Economic Zone (“SEZ”) to those wishing to develop fintech-related products from the jurisdiction.

The SEZ offers businesses focused on the fintech industry the opportunity to establish physical operations within the Cayman Islands in a more streamlined manner. It provides several benefits, including a simpler, more rapid, and cost-effective work permit process, concessions with respect to local trade licences and ownership requirements, the ability to be operational within four to six weeks, and allocated office space.

When coupled with the other benefits of the jurisdiction and its recently updated intellectual property laws, the SEZ has proven highly popular with the fintech industry, with the number of blockchain-focused companies established within it continuing to grow.

Ownership and licensing requirements

The Cayman Islands does not impose any restrictions or licensing requirements that are specifically targeted at the ownership, holding or trading of digital assets by those doing so for their own account.

As described above, under the VASP Law (once it is in force), all VASPs (as defined above) will be required to be licensed or registered with CIMA, obtain a waiver or hold a sandbox licence. The applicability of other regulatory regimes, such as the Mutual Funds Law and SIBL (each as further detailed above), should also be considered.

Pursuant to the VASP Law, a VASP will be required to ensure that its beneficial owners are approved by CIMA as fit and proper persons to have such control or ownership. Subject to possible exceptions for publicly traded companies, ownership interests or voting rights totalling 10% or more in a VASP cannot be issued or voluntarily transferred without CIMA's prior approval.

Mining

The mining of digital assets is not regulated or prohibited in the Cayman Islands currently, nor will it (in and of itself) be regulated or prohibited under the VASP Law. We would note, however, that the import duties applicable to computing equipment and the high cost of electricity production in the Cayman Islands are likely to present practical deterrents to the establishment of any material mining operations within the jurisdiction. It is possible that the increased availability of renewable energy options, and the falling price of the same, may mitigate this somewhat in the future.

Border restrictions and declaration

The Cayman Islands does not impose any general border restrictions on the ownership or importation of digital assets.

As part of the Cayman Islands' commitment to combatting money laundering and terrorist financing, the Customs (Money Declarations and Disclosures) Regulations mandate that individuals transporting money amounting to C\$15,000 (approximately US\$18,292) or more into the Cayman Islands must make a declaration in writing to customs officers at the time of entry. However, the Customs Law defines "money" as being confined to cash (i.e. bank notes or coins that are legal tender in any country) and bearer-negotiable instruments (i.e. travellers' cheques, cheques, promissory notes, money orders). As such, we would not expect such a requirement to apply to virtual assets or any other type of digital asset. Further, given the nature of these assets, particularly those based or recorded on a distributed ledger, there is a conceptual question of what would amount to the importation or transportation of such assets.

Reporting requirements

VASPs registered or licensed under the VASP Law will be required to:

- prepare audited accounts and submit them to CIMA annually;
- obtain prior approval from CIMA to appoint senior officers or AML compliance officers;
- provide certain notices to CIMA confirming compliance with AML Laws and data protection laws and ensuring that all communications relating to the virtual asset service are accurate;

- undertake audits of their AML systems and procedures at the request of CIMA; and
- notify CIMA of any licence or registration in another jurisdiction or the opening of an office or establishment of a physical presence in another jurisdiction, the holding or acquisition of a controlling interest in another person engaged in virtual asset service.

Additional reporting and other requirements may apply and may be imposed, which in some cases differ based on the type of virtual asset service being provided.

To the extent that any payment or transfer is made in the context of the conduct of a “relevant financial business” for the purposes of the AML Laws, there may of course be an obligation to make certain filings or reports in the event that there is a suspicion of money laundering or other criminal activity.

Estate planning and testamentary succession

Neither the VASP Law nor any other particular regime under Cayman Islands law deals specifically with the treatment of virtual assets upon the death of an individual holding them. This means that, in principle, and assuming Cayman Islands law governs succession to the deceased’s estate, virtual assets will be treated in the same way as any other asset and may be bequeathed to beneficiaries in a will, or, if a person dies intestate, will be dealt with under the intestacy rules in the Cayman Islands Succession Law.

As is the case in many jurisdictions beyond the Cayman Islands, there is likely to be some uncertainty as to where the *situs* of a virtual asset is located (or indeed whether or not a *situs* can be determined at all). To the extent that the asset can be analysed under traditional conflict-of-laws rules as sited in the Cayman Islands, then a grant of representation would be required from the Cayman Islands court to preclude the risk of intermeddling claims in dealing with the asset in the Cayman Islands.

The main potential difficulty that may arise is practical; namely that anyone inheriting a virtual asset will, on the face of it, often only be able to access that virtual asset if the personal representative of the deceased or the beneficiary (as the case may be) has or can obtain the information needed in order to gain access and control over that virtual asset (e.g. a private key to the wallet in which it is stored). Most exchanges have policies in place to transfer virtual assets to next of kin but these policies, and the transfer requirements, will vary between the exchanges.

**Alistair Russell****Tel: +1 345 749 2013 / Email: alistair.russell@careyolsen.com**

Alistair is a partner in the corporate and finance group of Carey Olsen in the Cayman Islands and advises on all aspects of finance, fintech, corporate, investment funds and commercial law.

He has advised clients on a broad range of transactions including financing, fintech, ICOs, private equity, joint ventures, mergers and acquisitions and capital markets, and is described by clients in *IFLR1000* as “the best Cayman lawyer we’ve ever worked with”.

Alistair was formerly with Skadden, Arps, Slate, Meagher & Flom and Cleary Gottlieb Steen & Hamilton, each in London.

Alistair obtained a Bachelor of Civil Law with distinction from Christ Church, University of Oxford, and an LL.B. with first-class honours from King’s College London.

**Jenna Willis****Tel: +1 345 749 2053 / Email: jenna.willis@careyolsen.com**

Jenna is an associate in the corporate and finance group of Carey Olsen in the Cayman Islands and advises on all aspects of finance, fintech, corporate law and restructuring and insolvency.

Jenna was formerly with Freshfields Bruckhaus Deringer in London and Blake, Cassels & Graydon in Toronto.

Jenna obtained a *Juris Doctor* with honours from Queen’s University, and a B.Sc. in Mathematical Science *summa cum laude* from McMaster University in Canada.

Carey Olsen

PO Box 10008, Willow House, Cricket Square, Grand Cayman KY1-1001, Cayman Islands

Tel: +1 345 749 2000 / Fax: +1 345 749 2100 / URL: www.careyolsen.com

Cyprus

Akis Papakyriacou
Akis Papakyriacou LLC

Government attitude and definition

At the moment, there is no comprehensive legal framework in place governing blockchain and cryptocurrencies; however, there have been positive steps towards establishing such framework. The Cyprus Securities and Exchange Commission (“CySEC”) has established an Innovation Hub which aims to act as a platform for both supervised and non-supervised entities to come together and share knowledge in order to accelerate their business models in line with the CySEC’s commitment to ensuring regulated entities’ investor protection. The CySEC via the Innovation Hub offers support to market participants who are introducing innovative financial products or services. On 10 February 2020, the CySEC issued a “*Report on the Activities of CySEC’s Innovation Hub*”, which essentially describes the objectives of the Innovation Hub and outlines any progress made thus far. The CySEC notes that the Innovation Hub attracted full-spectrum interest from both Fintech and Regtech companies, supervised entities and entities not subject to supervision, from Cyprus and abroad.

The Cyprus government, by a Council of Ministers’ decision N.85.629 dated 30 August 2018, has formed an *ad hoc* working group to develop and implement blockchain technology in Cyprus. The working group has established a national strategy and a roadmap for up to 2021. The priority in the national strategy is the enactment of a legal framework regulating blockchain and cryptocurrencies. Following the aforementioned decision N.85.629, three subcommittees of the working group were formed, namely: (a) a legal framework; (b) application in the public sector; and (c) application in the financial industry. The main objectives of the subcommittees are to (i) identify cases of public or private sector services that could be enhanced with Distributed Ledger Technology (“DLT”), (ii) develop guidelines and specifications that should be taken into account in the future development of the National DLT Services Infrastructure for it to support the deployment of the identified public sector use cases, and (iii) identify the parameters that should be included in the proposed regulatory framework. The national strategy aims to regulate, through a legal framework, cryptocurrencies and the trading of cryptocurrencies, assuming a categorisation of cryptocurrencies into Security Tokens and Non-Security Tokens. For the sake of clarity, Security Tokens can be described as a new version of a financial instrument, allowing fractionalised ownership of different assets; it is essentially a digital analogue of a traditional security such as shares. At the moment, we do not have a universal definition for Security Tokens; however, Security Tokens that confer analogue rights to those conferred by shares arguably fall under the definition of “transferable securities” under Article 1(1)(44) of MiFID II, and more specifically under sub-section (c) providing that “*any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures*” are deemed to be transferable securities.

On the other hand, Non-Security Tokens are unregulated tokens, which include Exchange Tokens and “cryptocurrencies” such as bitcoin. These tokens utilise a DLT platform, and they are not backed or issued by a bank or other central body. They do not confer the rights conferred by Security Tokens but are instead used as means for investment or exchange.

It is apparent that Cyprus is taking important steps to keep up with the international developments and trends by introducing new and innovative technologies applicable to financial services.

Cryptocurrency regulation

In Cyprus, there are currently no specific references to cryptocurrency in the legal or regulatory framework currently in force, and cryptocurrencies are not, *per se*, regulated, even though, as discussed in the previous section, positive steps have been taken toward the path of establishing a comprehensive legal framework. At the moment, such activities are regulated only to the extent that they fit in existing laws and regulations. Companies involved in activities or which offer services that relate to blockchain or cryptocurrencies are regulated only to the extent that their activities fall within the ambit of existing regulatory provisions. For the time being, even though there is no prohibition of cryptocurrencies, both the Central Bank of Cyprus (“CBC”) and the CySEC have issued a number of warnings to potential cryptocurrency investors as well as to investment firms (“CIFs”) looking to deal in, promote or provide cryptocurrencies.

To be more precise, on 7 February 2014, the CBC issued an announcement with the title “*Attentions to the risks associated with virtual currencies*”, whereby it highlighted that cryptocurrencies are not considered “*legal tender*”, noting also that any activity relating to cryptocurrencies is not authorised by the CBC, stressing that “*the public needs to be aware of the fact that there are no specific regulatory measures to cover losses from the use of virtual currencies if the platform that exchanges or holds them collapses and thus there is the risk of losing the entire amount deposited*”. The CBC also sets out therein, a non-exhaustive list of risks associated with cryptocurrencies, namely:

- There is a lack of guarantee or legal obligation to reimburse at face value.
- The price of virtual currencies is highly volatile; as a result, it may rise sharply or even fall to zero value.
- Any merchant may refuse to accept cryptocurrencies for payments.
- Transactions in cryptocurrencies are more likely to be misused for the purpose of illegal activities.

Along similar lines, the CySEC, on 6 February 2014, issued an announcement drawing the attention of the public, and particularly of potential investors, to the warning issued by the European Banking Authority (“EBA”) regarding the risks in connection with, or arising out of, the purchase, possession or trading of cryptocurrencies. Furthermore, the CySEC shared the report on the characteristics, functions and risks of virtual currency as issued by the European Central Bank.

Following the aforementioned announcement, the CySEC, on 18 March 2014, issued an additional announcement outlining, *inter alia*, the following risks associated when buying, holding, exchanging, or trading in cryptocurrencies:

- Cryptocurrencies deposited in an e-wallet could potentially be stolen.
- Transactions in cryptocurrencies could potentially involve money laundering and terrorist financing activities.

Subsequently, the CySEC, on 13 October 2017, issued a further announcement entitled “*Warning to investors on trading in virtual currencies*”, whereby it set out, *inter alia*, the following risks that could potentially arise when buying, holding, exchanging or trading in cryptocurrencies:

- Trading in cryptocurrencies or on contract for differences (“**CFDs**”) relating to cryptocurrencies is not suitable for all investors.
- There are no specific EU regulatory provisions that would protect existing and/or potential investors who trade on these products.
- Trading in cryptocurrencies comes with a high risk of losing all of the capital that has been invested.

In the same announcement, the CySEC stresses that investors must be very careful, particularly where they identify the following practices:

- “*Guaranteed high investment returns, with little or no risk;*
- *Unsolicited offers (without providing full analysis of the risks involved);*
- *Sounds too good to be true, as investments providing higher returns typically involve more (high) risks;*
- *Sales practices characterised by direct or indirect pressure or promises to actual or potential investors to trade in such products).*”

Furthermore, the CySEC stressed that “[i]nvestors should invest in an Initial Coin Offering [“**ICO**”] project if they have the necessary experience and knowledge, are confident of the quality of the ICO project itself and are prepared to lose their entire funds”.

On 15 May 2018, the CySEC issued Circular C.268 entitled “*Introduction of new rules governing derivatives on virtual currencies*” (the “**Circular**”) which has replaced Circular C.244 entitled “*Trading in virtual currencies and/or trading on contracts for differences relating to virtual currencies*”, issued by the CySEC on 13 October 2017. The Circular clarifies, *inter alia*, the following:

- Any activity relating to cryptocurrencies is not currently regulated by the CySEC.
- Derivatives on cryptocurrencies, however, are now capable of qualifying as financial instruments under the Law which provides for the provision of investment services, the exercise of investment activities, the operation of regulated markets and other related matters, L.87(I)/2017 (the “**Law**”). Among the financial instruments listed in Part III of the First Appendix of the Law, derivatives on cryptocurrencies may fall under the following:

- i. *[...] any other derivative contracts relating to securities [...] which may be settled physically or in cash;*
- ii. *financial contracts for differences;*
- iii. *[...] any other derivative contracts relating to assets [...] not otherwise mentioned in this Section, which have the characteristics of other derivative financial instruments.*”

“*Therefore, depending on their specific characteristics and use, providing investment services in relation to derivatives on virtual currencies will require specific authorisation by CySEC.*”

The Circular also outlines the obligations of CIFs when providing investment services in derivatives on cryptocurrencies. Specifically, the Circular sets out the following non-exhaustive list of obligations:

- “*act honestly, fairly and professionally, in accordance with the best interests of their clients;*
- *provide fair clear and not misleading information to their clients;*

- *provide appropriate guidance on and warnings of the risks associated with investments in those instruments;*
- *have adequate product governance arrangements;*
- *execute orders on terms most favourable to the client;*
- *maintain adequate capital.”*

The Circular further provides the following:

- CIFs must consider the product governance requirements when manufacturing, designing, and/or distributing derivatives on cryptocurrencies.
- CIFs must provide the investors or potential investors with all information including, but not limited to, the risks associated with the derivatives on cryptocurrencies and fees and costs.

Moreover, it is provided that CIFs:

- should ensure that the reference prices used are gathered from publicly available sources of good repute;
- shall consider the risks associated with derivatives on cryptocurrencies in the context of their internal Capital Adequacy Assessment (“ICAAP”); and
- shall consider the European Securities and Markets Authority (“ESMA”) intervention measures and leverage limits.

Taking into account the above, in conjunction with ESMA’s (i) Press Release dated 13 November 2017 with respect to ICOs, and (ii) Advice on ICOs and Crypto-Assets, where ICOs qualify as financial instruments, it is likely that companies involved in ICOs are essentially conducting regulated investment activities, and would therefore need to comply with the relevant legislation, indicatively: the Prospectus Directive; MiFID II; the Alternative Investment Fund Managers Directive (“AIFMD”); and the Anti-Money Laundering Directive (and the corresponding national legislation).

Sales regulation

ICOs have become increasingly popular as a way of raising funds. It is very common for cryptocurrencies to be used in an ICO. There is no prohibition on ICOs in Cyprus; however, care needs to be taken in order to ensure that the way in which an ICO is conducted does not cause a breach of any relevant regulatory framework. For example, an Alternative Investment Fund with Limited Number of Persons would potentially be an appropriate vehicle for such ICOs to take place in Cyprus, as there are no diversification requirements and it is a relatively flexible investment vehicle.

Taxation

Any funds that derive from an ICO are subject to tax in Cyprus as they are deemed to be taxable income; however, Cyprus has one of the lowest and most attractive corporate tax rates at 12.5%. With respect to the value-added tax (“VAT”) treatment of ICOs, it is noted that at the moment, the guidance with respect to the VAT treatment of cryptocurrencies is limited, and most of it comes from the European Court of Justice judgment of case C-264/14 *Hedqvist* which provided the basis for the VAT treatment of transactions concerning the exchange of traditional currencies for bitcoins and *vice versa*, noting that these are exempt from VAT. On the matter of Security Tokens, based on their function these may be deemed to be equity or debt liability and may therefore be excluded from both corporate tax and VAT.

Money transmission laws and anti-money laundering requirements

The CySEC, on 19 February 2019, issued a Consultation Paper with respect to the proposed amendment of the Prevention and Suppression of Money Laundering and Terrorist Financing Law 188(I)/2007 to 2019 (the “**AML Law**”) for the prevention and suppression of money laundering and terrorist financing.

The proposed amendments intend to extend the scope of the AML Law by applying the AML Law obligations to the use of cryptocurrencies.

This Consultation Paper concerns entities engaging in the following activities/services in relation to cryptocurrencies:

- *“exchange between cryptocurrencies and fiat currencies;*
- *exchange between one or more forms of cryptocurrencies;*
- *transfer of cryptocurrencies;*
- *custodial and/or administrative services related to cryptocurrencies or instruments enabling control over cryptocurrencies;*
- *participation in and provision of financial services related to an issuer’s offer and/or sale of cryptocurrencies.”*

Additionally, this Consultation Paper concerns customers who are purchasing, holding or transferring cryptocurrencies.

In the Consultation Paper, the CySEC, in line with ESMA’s guidance on ICOs and cryptocurrencies, has stressed that money laundering is one of the most significant risks identified. The CySEC, like ESMA, is of the view that all cryptocurrencies and related activities should be subject to AML Law provisions.

The CySEC has commented that since the launch of the Innovation Hub, numerous entities engaging in activities involving cryptocurrencies have contacted them, noting that a number of these entities do not fall within the existing legal and regulatory framework. Therefore, the CySEC considers it imperative to proceed with the transposition of the parts of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 (the “**AMLD5**”) concerning the following activities:

- *“exchange services between virtual currencies and fiat currencies;*
- *the custodian wallet providers’ activities.”*

In the Consultation Paper, the CySEC proposes the definition deriving from the AMLD5 and seeks consultation on the merits of creating an all-encompassing definition of “*virtual assets*”, which would include the definition of “*virtual currencies*” as provided in the AMLD5 and the definition of “*virtual assets*” as provided by the Financial Action Task Force.

The CySEC has also proposed extending the scope of the AML Law in order to go even beyond the provisions of the AMLD5 and include the following activities and services:

- *“exchange between crypto assets and crypto assets,*
- *transfer of virtual assets, and*
- *participation in and provision of financial services related to an issuer’s offer and/or sale of a crypto asset.”*

Promotion and testing

The CySEC has established an Innovation Hub to foster a better, more effective relationship between entities operating, *inter alia*, in the areas of cryptocurrencies and blockchain. Further to the CySEC’s initiative to set up the Innovation Hub, the Cyprus government has also taken the first steps towards the implementation of blockchain technology in

Cyprus, through the formation of an *ad hoc* working group. A more extensive account of the objectives and actions of the Innovation Hub and of the *ad hoc* working group is given in the “Government attitude and definition” section above.

Ownership and licensing requirements

Currently there is no specific restriction and/or licensing requirement under Cyprus law.

Mining

Currently there is no specific restriction and/or licensing requirement under Cyprus law.

Border restrictions and declaration

Currently there is no specific restriction under Cyprus law.

Reporting requirements

Reporting requirements apply only to derivatives on cryptocurrencies.

Estate planning testamentary succession

At the moment, there is no legal framework, regulation and/or guidance as to how testamentary succession of cryptocurrencies should be treated. We have therefore made the assumption that the treatment of cryptocurrencies would be the same as the treatment of any other movable property in Cyprus.

Subject to the provisions of EU Regulation 650/2012, the Wills and Succession Law Cap 195 regulates wills and intestacy; it applies to the estate of any deceased person with a Cyprus domicile, and to all immovable property located in Cyprus. That is, Cyprus succession laws will apply to movable and immovable property of a person domiciled in Cyprus, and to Cyprus-*situs* immovable property irrespective of the deceased’s domicile at the time of death. It is noted that is not obligatory for a will to be made and, in the absence of a will, the property is distributed on the basis of Cyprus succession laws.

It should be noted that even where there is a will, there are restrictions with respect to the manner in which property can be disposed of. Cyprus succession laws implement a forced heirship regime which means that certain relatives, such as a spouse or children, cannot be excluded from an inheritance and they have a right to a fixed minimum percentage of the estate. It should be noted that forced heirship regime applies to everyone who dies domiciled in Cyprus, regardless of nationality; however, EU citizens are conferred the rights by EU Regulation 650/2012 to choose the law of their country of nationality as the law applicable to their estate; in such case, it should be expressly provided for in the will. Where the deceased leaves no spouse, child or descendant of a child, the rules of forced heirship do not apply and 100% of the estate of the deceased who is domiciled in Cyprus may be disposed of freely by will.

The above description of Cyprus succession laws is made on the assumption that the treatment of the succession of cryptocurrencies will be the same as for movable property in Cyprus. We have no other indication thus far as to how the succession of cryptocurrencies will be treated once a legal framework is formed.

**Akis Papakyriacou****Tel: +357 22 256 882 / Email: akis@papakyriacoulaw.com**

Akis graduated from the University of Salford with first class honours (LL.B.) and obtained his M.Sc. from the University of Oxford (Corpus Christi). Akis attended the City Law School where he passed the Bar Professional Training Course (Very Competent). Following the completion of his studies, Akis returned to Cyprus to complete his vocational training in one of the leading law firms, where he continued working after the completion of his training, specialising in corporate, banking and finance law until September 2018. Prior to forming Akis Papakyriacou LLC, Akis worked as a partner in a law firm in Nicosia.

Akis focuses on corporate, banking and finance transactions, with experience in both local and international finance transactions. His knowledge and expertise also extend to merger and acquisition transactions, corporate restructurings, employment law matters and fund-related matters.

Akis Papakyriacou LLC

1 Dimofontos Street, Exsus Business Centre, Lamda Tower, 6th Floor, 1075 Nicosia, Cyprus

Tel: +357 22 256 882 / URL: www.papakyriacoulaw.com

Gibraltar

Joey Garcia & Jonathan Garcia
ISOLAS LLP

Government attitude and definition

The Government of Gibraltar has approached the growing cryptocurrency and wider blockchain and distributed ledger technology (“DLT”)-related sector with a uniquely receptive and progressive attitude. Financial regulators and policymakers in Gibraltar have understood the need for regulation in this sector, responding rapidly to such demand as far back as 2014, with the creation of the Cryptocurrency Working Group. This private sector initiative led to the development of the Distributed Ledger Technology Framework (“DLT Framework”), which became effective on 1 January 2018, making Gibraltar the first jurisdiction in the world to deliver a framework of its kind that regulates businesses that use DLT for the defined purposes relating to a “storage” or “transfer” of “value”, which is a wider concept than pure virtual assets. The DLT Framework currently includes nine principles that apply to DLT businesses operating in Gibraltar and these principles are substantiated by detailed guidelines constructed in a way that allows them to evolve at the same pace as the technology and its application, while always maintaining the core regulatory and legislative principles. The response to this approach has been global and truly significant. Those who know nothing about Gibraltar may be surprised, but those who know the history of the small jurisdiction, with a joined-up partnership between lawmakers, regulators and industry that is able to adapt and evolve to attract the right opportunities at the right level, with the speed and flexibility needed to accomplish such goals, will not be surprised at all. This success has also been seen in the crypto funds space. A recent report into the global crypto hedge fund landscape from PwC and Elwood Asset Management has shown Gibraltar as the third-highest jurisdiction of choice for crypto hedge fund managers, only behind the US and UK. Gibraltar, which is also listed as having the fourth-highest number of domiciled crypto hedge funds, puts the jurisdiction ahead of financial centres such as Hong Kong, Malta, the Netherlands, Singapore, Switzerland and many others, despite its relative size.

Since the coming into force of the DLT Framework, the Government of Gibraltar has been delivering on a detailed and strategically formulated activity schedule, created to proactively drive home Gibraltar’s very strong DLT message, by researching and identifying key markets and audiences and focusing its marketing in these areas. The Gibraltar Government also launched an advisory group that focuses on the creation of new technology-related education courses, such as blockchain. The New Technologies in Education (“NTiE”) group is a joint initiative between the Government and the University of Gibraltar in collaboration with some of the leading new technology companies based in Gibraltar. The advisory group’s aim is to address the growing demand for related skills as the sector continues to expand in Gibraltar. The University of Gibraltar is currently running a professional course in this space titled “Professional Certificate of Competence in Blockchain & Smart Contracts”.

Whilst Gibraltar has shown leadership in this space, development is clearly an ongoing process and Gibraltar is aware of the importance, as a jurisdiction, for it to invest in supporting the development of knowledge and skills in tandem with generating economic results as it continues to strive for excellence. The Gibraltar Government created the Gibraltar Association for New Technologies (“GANT”), an association formed together with the private sector, including Gibraltar’s leading law firms, accounting firms and technology companies all forming part of its membership. GANT serves several purposes, primarily enhancing the development in Gibraltar of the use of blockchain and DLT and other future developments (collectively referred to as “New Technology”), with a view to enhancing the reputation, integrity and public trust in this sector.

GANT has also been tasked to raise the profile of “New Technology” in Gibraltar across a spectrum not necessarily limited to financial services. This includes encouraging respective organisations to emphasise the high value of their reputation and interest in contributing to enhanced client and investor protection and remaining committed to safeguarding customer and jurisdictional interests. GANT also provides a forum for discussion on “New Technology” issues within the membership and to assist other sectors of the wider Gibraltar Finance Centre, whilst also assisting and advising the Gibraltar Government on all aspects of this sector.

Cryptocurrency regulation

In terms of the activity of the business in the DLT space, as highlighted above, Gibraltar has developed the first DLT-specific regulatory and principles-based legislative framework for these operators. This detailed framework goes well beyond the basic compliance requirements or registration processes that exist in many jurisdictions. Cryptocurrencies are not considered legal tender in Gibraltar and, accordingly, are not issued or guaranteed by the Gibraltar Government. However, as in most jurisdictions that operate under European law principles, depending on the construct of the virtual currency, they may still qualify as electronic money (“E-Money”), as a form of asset-backed security, financial instrument or even unit of a collective investment scheme (“CIS”) arrangement. Without being able to go into each of these for the purposes of this chapter, in the context of the recent focus on stablecoins and central bank-issued digital currencies, on a European level, the regulation of E-Money is based on the EU E-Money Directive, which defined E-Money as an electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions, and accepted by a natural or legal person other than the E-Money-issuer. This definition is in line with the definition contained in the Financial Services (Electronic Money) Regulations 2020 which transposes the E-Money Directive into Gibraltar law. E-Money requires an issuer. Therefore, a cryptocurrency that comes into existence by way of mining (e.g. Bitcoin) without an issuer, or representing any form of claim on any issuer, should not qualify as E-Money. Conversely, a cryptocurrency that is issued by an issuer at par value against fiat and furnished with the promise of the issuer to be redeemed in exchange for fiat against the issuer of that currency, and therefore being accepted as means of payment by third parties, would qualify as E-Money and trigger a number of considerations around this from a payments services perspective also.

Owing largely to the difficulty of regulating cryptocurrencies themselves, the DLT Framework has attempted not to enforce the regulation of cryptocurrencies, but instead to impose a regulatory regime for firms that carry on by way of business, in or from

Gibraltar, the use of DLT for storing or transmitting value belonging to others. Accordingly, regulation will depend on what services a firm is providing customers in respect to their cryptocurrencies and whether this falls under the scope of regulation.

Because cryptocurrencies vary widely in design and purpose, it should be kept in mind that these may represent transferable securities or financial instruments, and their promotion and sale would already be covered by existing securities legislation in Gibraltar such as the Financial Services Act 2019. Its classification as a security triggers various consequences; in particular, regulatory consequences. The requirement to issue a prospectus when offering securities publicly is only one example of such a requirement. A distinction must be drawn between the concept of a security on the one hand and a financial instrument on the other, with the latter being the broader term.

“Securities” are one of several sub-categories of financial instruments. Regulatory requirements may therefore also arise for non-securities that are classified as financial instruments. This includes the requirements arising under MiFID II, transposed into Gibraltar law through the Financial Services Act 2019 and the Financial Services (Investment Services) Regulations 2020, which, in addition to applying to businesses providing certain investment services or engagement in certain activities with clients in relation to financial instruments, also defines “financial instruments” in a wide form, including forms of commodity derivative contracts and arrangements that may apply to any asset or right of a fungible nature (under certain conditions).

If a cryptocurrency meets the MiFID II definition of a financial instrument, then a number of crypto-asset-related activities carried out by an exchange are likely to qualify as investment services/activities for which a licence is required outside of the DLT Framework. This includes multilateral trading facilities (“MTF”), organised trading facilities (“OTF”) and other exchange-related activities.

Gibraltar is further looking to expand and extend the obligations to which DLT firms must adhere and is subsequently looking towards adding a 10th principle to the DLT Regulations with an aim to regulate and develop market integrity standards for crypto exchanges. The International Organization of Securities Commissions (“IOSCO”) has identified several issues that merit consideration relating to transparency, custody, clearing and settlement trading, security and systems integrity. Implementing market integrity standards for these exchanges is one of the most pressing issues in the market, with organisations such as Bitwise and BTI estimating that 70–95% of all trading volume on exchanges is potentially manipulative. The effect of which is a reduction in market confidence in this sphere.

It should of course be borne in mind that foreign exchange markets, stock markets and commodity brokers face or have faced market risks in the past, but now fall squarely within developed rules and frameworks that prevent or restrict such manipulation taking place. This is not to say that there is no manipulation taking place in the more mainstream markets, but rather that it is less prevalent due to such regulation. Thus, the introduction of these standards in the regulatory sphere in Gibraltar would serve to restrict manipulation in the same way that this is restricted in traditional markets.

The effect of manipulation serves no purpose other than to reduce market confidence in the space and thus it is hoped that the introduction of market integrity standards will not only serve to curtail the amount of manipulated trading volume, but will do so whilst ensuring that DLT exchanges are not overburdened by onerous regulatory controls.

Sales regulation

It may be the case that tokens do not qualify as securities or financial instruments under Gibraltar or EU legislation. Gibraltar also does not maintain separate classifications of virtual asset categories but, although the issuance of any token may not be captured within Financial Services legislation, from a compliance and risk perspective, any such creation and issuance will always be caught by the Proceeds of Crime Act (“POCA”) in Gibraltar which was specifically amended to capture this activity. Similarly, the operation of the actual business relating to such a token or virtual asset could also be captured within the DLT Framework, despite the issuance potentially not being captured. In the event that the token or assets do constitute securities, there is currently an EU-wide framework dealing with this, as has been described above. Accordingly, Gibraltar is not looking to introduce a framework that will modify, in any way, securities law or the EU Prospectus Regulation requirements. That is to say, the public offering of tokens that constitute securities does not require further regulation from a Gibraltar perspective and will continue to fall under current frameworks governing the issuance of securities.

It should also be noted that entities issuing tokens may separately have to comply with classic consumer protection law, depending on the design of the digital token. All relevant EU legislation covering e-commerce and consumer protection has been transposed into Gibraltar law via various Acts of Parliament or Regulations. The EU e-commerce and consumer protection rules (E-Commerce Directive, Consumer Rights Directive, Directive on Distance Marketing of Consumer Financial Services) all specify the information that should be disclosed.

Taxation

It should be noted that the treatment of cryptocurrencies is not specifically considered in current tax legislation in Gibraltar, nor in accounting standards that are generally accepted in Gibraltar; therefore, where relevant, general principles implicit in current legislation, and accounting standards that are believed to be appropriate, are applied.

In Gibraltar, there is no capital gains tax, value-added tax, death duties, inheritance, wealth, capital transfer, gifts, or withholding tax levied at present. For companies, corporation tax is generally 10%, payable on profits that derive from income accrued in or derived from Gibraltar; that is to say, by reference to the location of the activities that give rise to the profits. Under tax legislation, the location of the activities that give rise to the profits of a business whose underlying activity results in income, and requires a licence and regulation under any law of Gibraltar, shall automatically be considered to derive from Gibraltar. Favourable tax packages are also available for High-Net-Worth Individuals and High Executives Possessing Specialist Skills who want to establish residence in Gibraltar and can benefit from tax payable on income being restricted to a capped amount, which encourages talent toward Gibraltar.

Money transmission laws and anti-money laundering requirements

A DLT firm is caught as a relevant financial business under POCA in Gibraltar. Accordingly, a DLT firm is subject to know your customer (“KYC”) and anti-money laundering (“AML”) obligations. Furthermore, under the DLT Framework, a DLT firm “must have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing”. The requirement is derived from: EU Anti-Money Laundering Directives; POCA 2015; and the FFSC0 Anti-Money Laundering Guidance Notes. There

are also additional and specific guidance notes relating to the “Financial Crime” factor which have been prepared specifically for DLT firms to set out regulatory expectations.

Firms are required to establish procedures to: apply customer due diligence (“CDD”) procedures; appoint a Money Laundering Reporting Officer (“MLRO”) to whom money laundering reports must be made; establish systems and procedures to forestall and prevent money laundering; provide relevant individuals with training on money laundering and awareness of their procedures in relation to money laundering; screen relevant employees; and undertake an independent audit for the purposes of testing CDD measures, ongoing monitoring, reporting, recordkeeping, internal controls, risk assessment and management, compliance management and employee screening. The frequency and extent of the audit shall be proportionate to the size and nature of the business.

It is possible for a DLT firm’s compliance programme to use customer verification tools (such as Jumio) as well as blockchain technology (such as Coinfirm). As the DLT Framework is based on the application of principles rather than rigid rules, DLT firms are able to use innovative solutions provided they can satisfy the Gibraltar Financial Services Commission that they meet its regulatory obligations.

The application of this AML regime to DLT firms has been seen by many as a precursor to the requirements under the EU’s Fifth Anti-Money Laundering Directive (“AMLD5”) which has, for the first time, captured exchanges and pure custody wallet providers. Gibraltar-based businesses were already fully regulated and subject to such requirements as implemented by AMLD5 since the introduction of the DLT Framework, and so the introduction of AMLD5 has had no significant effect on those businesses operating from Gibraltar.

Promotion and testing

Gibraltar has always maintained itself at the forefront of novel technological development. In fact, for most online gambling businesses around the world, it is found that most are based in Gibraltar which was also the fastest mover in developing regulation around that space.

Gibraltar is hoping to replicate that philosophy in the blockchain space and follow the success of online gaming, and is doing so by stepping out of the regulatory “sandbox”, in the same way as it did back in the gaming days. Rather than creating a “safe space” for businesses to test innovative financial products, services, business models and delivery mechanisms in a live environment without immediately incurring all the normal regulatory consequences of engaging in the activity in question, Gibraltar has instead chosen to provide legal certainty and allow businesses to operate within a purpose-built legislative framework. In doing so, it considers that a flexible, adaptive approach is required in the case of novel business activities, products and business models and that whilst regulatory outcomes remain central, these are better achieved through the application of principles rather than rigid rules. This is because, for businesses based on rapidly evolving technology, such hard and fast rules can quickly become outdated and unfit for purpose. Accordingly, Gibraltar’s principles-based framework is based on risk and proportionality, and is outcome-focused yet robust.

The Gibraltar Government recognises that this is a nascent industry and whilst Gibraltar has shown leadership in this space, development is clearly an ongoing process and Gibraltar is aware of the importance, as a jurisdiction, for it to invest in supporting the development of knowledge and skills, in tandem with generating economic results as Gibraltar continues to strive for excellence.

Ownership and licensing requirements

If a firm is engaging in an activity for business purposes, which involves the storage or transmission of cryptocurrencies belonging to third parties, it will need to be authorised under the DLT Framework.

If there is an intention to establish an arrangement that enables a number of investors to pool their assets and have these professionally managed by an independent manager, rather than buying investments directly as individuals, then CIS law is another relevant legal consideration.

The Financial Services Act 2019 defines a CIS as “any arrangement with respect to property, the purpose or effect of which is to enable persons taking part in the arrangement, whether by becoming owners of the property or any part of it or otherwise, to participate in or receive profits or income arising from the acquisition, holding, management or disposal of the property or sums paid out of such profits or income”.

The arrangement referred to above must be such that the participants in the arrangement do not have day-to-day control over the management of the assets. Further, the investments and the profits/income arising from them must be pooled, and/or the property managed as a whole.

There are two popular structures for setting up a CIS in Gibraltar: the Experienced Investor Fund (“EIF”); and the Private Scheme (“PS”). These structures are agnostic to the underlying assets they govern for investors.

Typically, a CIS that is to focus on crypto-assets would best be established as an EIF. Only when such a CIS is set up for a small group of persons previously known to each other, and where there will be no promotion of the CIS, would it be suitable to set up a CIS of this nature as a PS. Indeed, the local Gibraltar Funds and Investment Association (“GFIA”) has recently published a draft code of conduct to this effect which also serves as a reference point of elements that should be kept in mind when establishing funds dealing with crypto-assets. Among other things, the code will cover custody of crypto-assets, valuation, corporate governance and security.

The EIF is designed for professional, high-net-worth or experienced investors. Each investor would need to invest at least €100,000 in the EIF – or its equivalent in an alternative fiat – or prove a net worth of at least €1m, excluding one’s personal residence.

The EIF regime is reliant on EIF Directors and other licensed service providers.

A CIS of this nature will fall within the definition of an alternative investment fund (“AIF”) under the Financial Services (Alternative Investment Fund Managers) Regulations 2020, which transposes the EU Alternative Investment Fund Managers Directive. Accordingly, there will be multiple considerations that become relevant, both in terms of the sale, promotion and management of that AIF, as well as the depositary arrangements for AIF units.

Mining

The mining of Bitcoin and other cryptocurrencies is not covered by any specific legal or regulatory framework. Accordingly, it is permitted. As set out above, a cryptocurrency such as Bitcoin, which comes into existence by way of mining without an issuer, does not qualify as E-Money. However, this will ultimately depend on how the mining activity is conducted. For example, given the definition of an AIF, if the mining activities are conducted in a particular way that involves a collective group of people and shared infrastructure, an argument could certainly be made that the arrangement would qualify as a collective undertaking in the sense of the legal meaning.

Border restrictions and declaration

Presently, there are no border restrictions in place on declaring cryptocurrency holdings. Instead, these restrictions are usually in place for issues such as transport of goods. Though there are no restrictions in this sense, several of the above authorisation processes required by the regulations will require “mind and management” to be in Gibraltar, comprising an office with registered employees.

Reporting requirements

No specific reporting requirements are triggered for cryptocurrency payments made in excess of a certain value. However, any threshold amounts may determine the recordkeeping requirements that may apply to a business under POCA. Businesses under POCA must report suspicious activity of money laundering.

However, it is worth noting that in October 2018, the Financial Action Task Force (“FATF”) amended its Recommendation 15 (New Technologies) of its 2012 Recommendations on International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation (the “FATF Standards”) to explicitly clarify that the FATF Standards apply to financial activities involving “virtual assets” and added two new definitions relating to “virtual assets” and “virtual asset service providers” (“VASPs”). The FATF also began working on an Interpretative Note to Recommendation 15 to clarify the FATF Standards that apply to virtual assets and VASPs (the “INR 15”), as well as Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (the “VASP Guidance”), which explains how the FATF Standards apply to virtual assets and VASPs on a Recommendation-by-Recommendation basis.

Both the INR 15 and VASP Guidance were adopted by the FATF in June 2019, and clarified how the FATF Standards should apply, in particular in respect of the application of a risk-based approach to virtual asset activities and VASP operations, with supervision or monitoring for AML and combatting the financing of terrorism (“CFT”) purposes, licensing or registration, preventative measures such as CDD, recordkeeping, suspicious transaction reporting and other sanctions and enforcement measures.

Without wishing to go into too much detail, it is important to note that while many jurisdictions took a reactive approach to the VASP Guidance and INR 15, beginning to take steps to comply with them after they were adopted in June 2019, Gibraltar had such measures in place since January 2018, well before the FATF introduced its VASP Guidance. Furthermore, in our view, Gibraltar’s DLT Framework goes well beyond the FATF Standards in respect of the licensing and registration of VASPs. As a simple example, the VASP Guidance suggests that VASPs should be required to meet “*registration criteria set by relevant authorities*”. The wording at paragraph 80 cites the fact that Authorities should:

“[...] impose such conditions on licensed or registered VASPs to be able to effectively supervise the VASPs. Such conditions should allow for sufficient supervisory hold and could potentially include, depending on the size, nature of the VASP activities, requiring a resident executive director, substantive management presence or specific financial requirements.”

Estate planning and testamentary succession

The law of succession in Gibraltar is largely based upon the UK Wills Act 1837, which is amended by Gibraltar’s Wills Act. Administration of estates is governed by Gibraltar’s Administration of Estates Act 1933, consolidated in 1948 (as amended).

The law of Gibraltar as it relates to a deceased person who dies domiciled, closely resembles the laws of England & Wales. Moveable and immoveable property are treated differently. In the case of moveable property, the law of the country where the deceased died domiciled is applied.

There are no death duties to pay in Gibraltar.

Estate planning for cryptocurrency presents its own unique difficulties. Ordinarily, probate is a public process completed upon the presentation of various legal documents. Both of these concepts are in conflict with cryptocurrency.

Estate practitioners are going to have to be aware of the specific issues of cryptocurrency when drafting testaments, the aim being to ensure that the cryptocurrency property is accurately reflected, can be properly transferred upon the death of the holder, and also to ensure that the value of the property can be maintained.

As yet, there is no specific guidance issued in Gibraltar in relation to cryptocurrency and estate planning or succession.

**Joey Garcia****Tel: +350 2000 1892 / Email: joey.garcia@isolas.gi**

Joey Garcia is a corporate and fintech lawyer at ISOLAS LLP. He co-chaired the government's working group on blockchain to develop the infrastructure to accommodate a DLT regulatory framework in Gibraltar and was recognised as one of the top 12 lawyers in the world in this space. He is a member of the prestigious global Wharton Reg@Tech think tank in Philadelphia, a founding member of the European think tank thinkBLOCKtank, and a member of the Digital Chamber of Commerce in Washington. Joey is also part of the UNODC cryptocurrencies technical experts' workshop and contributed to the first book on blockchain and cryptocurrency regulation for 2019. He is a Xapo representative on the Libra Association and part of the Policy and Regulatory working group with Libra. He is also the appointed lecturer at the University of Gibraltar and the vice chair of the Gibraltar Association for New Technologies.

**Jonathan Garcia****Tel: +350 2000 1892 / Email: jonathan.garcia@isolas.gi**

Jonathan Garcia is a partner at ISOLAS LLP in the DLT/Fintech & Financial Services Team and is the other partner, alongside Joey Garcia, who heads the team. Jonathan specialises in financial services, specifically advising collective investment schemes, investment managers, banks, e-money institutions and blockchain start-ups on licensing and regulatory matters. He has over 10 years of experience as a financial services lawyer and spent six months on a part-time secondment at the Gibraltar Financial Services Commission. Jonathan is part of the board of the Gibraltar Funds and Investment Association (GFIA), the local body that represents the funds and investments industry, and sits on various government/regulator working groups dealing with a variety of issues. Most recently, he is participating in a working group on the Prospectus Regulations. The aim of this working group is to cover legal derogations and how best to apply the requirements in Gibraltar.

ISOLAS LLP

Portland House, Glacis Road, GX11 1AA, Gibraltar
Tel: +350 2000 1892 / URL: www.gibraltarlawyers.com

Hong Kong

Yu Pui Hang (Henry Yu)
L&Y Law Office / Henry Yu & Associates

Government attitude and definition

Cryptocurrencies (often called “coins” or “tokens”, and collectively referred to in a colloquial manner as “crypto”) and blockchain technology (certain blockchain technologies may also be referred to as “Distributed Ledger Technology” or “DLT” for short) have, in their short life span of the past decade, created a new economy which opened a market of new opportunities.

The first cryptocurrency to enter the market was Bitcoin, and it has introduced an effective way to transfer value over the internet by relying on peer-to-peer and distributed verification. Ever since Bitcoin, there have been other blockchain-based projects that have introduced new innovations to blockchain technology (these cryptocurrencies are often referred to as “Altcoins”), one of the most noteworthy being Ethereum, which allows for the deployment and execution of software on the blockchain called smart contracts. As a result of this growth, many private and public enterprises have formed in Hong Kong to take advantage of the opportunities offered by this new technology, and to leverage Hong Kong’s unique position in business, technology and law.

Hong Kong is a unique jurisdiction, as it leverages the “one country, two systems” principle, which gives it a high degree of autonomy. The Basic Law of Hong Kong enshrines various free market principles, safeguarding its position as an international financial centre. Thus, given its free market foundations, the legislative council in Hong Kong has yet to pass any new laws and regulations that specifically deal with cryptocurrencies or cryptocurrencies business. However, the rapidly expanding cryptocurrencies or cryptocurrencies businesses market caught the Hong Kong government’s attention, resulting in enforcement actions being taken under the existing legislation and new regulatory regimes being introduced with the goal of better protecting investors’ interests.

As there is no new primary legislation to directly regulate cryptocurrencies in Hong Kong, there is a certain degree of uncertainty on the legal definition within the statutory law. Nevertheless, there are secondary sources of law, including the designation set by the Secretary for the Financial Services and Treasury Bureau (“FSTB”), Professor K C Chan, who designated Bitcoin (specifically) as a “virtual commodity”. In a press release, the Hong Kong Monetary Authority (“HKMA”) stated in 2015 that Bitcoin and other similar currencies were not legal tender but “virtual commodities”, and as Bitcoin has no backing – either in physical form or by the issuers – it cannot be qualified as a means of payment or electronic money. The HKMA, which acts as Hong Kong’s *de facto* central bank, has also stated that it has no plans to issue any central bank-backed cryptocurrency. On the other hand, the Hong Kong Securities and Futures Commission (“SFC”) had issued a number of statements in 2018 and 2019 in an attempt to monitor the activities involving

cryptocurrency, including a statement dated 1 November 2018 titled “Statement on Regulatory Framework for Virtual Asset Portfolios Managers, Fund Distributors and Trading Platform Operators” (the “2018 SFC Statement”) and a statement dated 28 March 2019 titled “Statement on Security Token Offerings” (the “2019 SFC Statement”), both of which gradually show the Hong Kong government’s stance towards cryptocurrency and cryptocurrency businesses. Interestingly, in the 2018 SFC Statement, the concept of a new asset class called “virtual assets” was introduced, which refers to “a digital representation of value” (the “Virtual Assets”), and examples include “cryptocurrencies”, “crypto-assets”, “digital tokens” and “digital tokens (such as digital currencies, utility tokens or security or asset-backed tokens) and any other virtual commodities, crypto assets and other assets of essentially the same nature”. This seems, to a certain extent, to expand on the HKMA’s categorisation of “virtual commodities”.

The most observable attitude made by the government and the various regulatory authorities is to warn the public against the uncertainties in the cryptocurrency marketplace. The earliest observable public warning was made by the Hong Kong Police Force in 2014 which highlighted that Bitcoins are not money and are not regulated by the HKMA; the volatility of the prices of Bitcoin; the cybersecurity risks associated with dealing with Bitcoin; and any potential fraud especially with “Bitcoin Mining Contracts”. Any suspected proceeds of crime should be reported to the Joint Financial Intelligence Unit (“JFIU”), a joint unit composed of the Hong Kong Police Force and the Hong Kong Customs and Excise Department (“CED”). The press release issued by the HKMA, as referred to above, contained a similar warning about the volatile nature of Bitcoins.

With the advent of Ethereum and other smart contract blockchain platforms, new applications of cryptocurrency such as initial coin offerings, or token sale (collectively “ICO(s)”), become more widely popular in Hong Kong and globally. As many ICO issuers have established their base of operations in Hong Kong and have opened their campaigns to Hong Kong residents, the SFC, the local securities regulator, has issued a statement on ICO on 5 September 2017 warning the public about: (i) the risk of participating in ICO campaigns; (ii) that ICO tokens that possess features of “securities” as defined under the Securities and Futures Ordinance (Cap. 571) (the “SFO”) would require to be authorised by the SFC, unless an exemption applies; and (iii) that dealing and advising on “securities”-based ICOs would be a “regulated activity” under the SFO and therefore such activity should only be carried out by licensed corporations.

In subsequent public communications, the SFC has stated that it is monitoring the cryptocurrency space and will enforce any relevant provision under the SFO if necessary. Aside from the statements given by the SFC, in early 2018 the Investor Education Centre and the FSTB launched an education campaign on ICOs and cryptocurrencies. The campaign’s key message is not to buy something you do not understand. We can therefore see that, the Hong Kong government’s view towards cryptocurrencies, that do not possess features of securities, can be described as relatively passive. The regulatory authorities have not called for new legislation to regulate cryptocurrencies, as current laws are still applicable. For now, it is observable that the government and the regulatory authorities aim to educate the public about the risks involved in the cryptocurrency economy and still assessing the suitability of the currently available legislation in regulating cryptocurrencies and protecting the public.

Notwithstanding the above, in 2018, the cryptocurrency economy saw the introduction of security token offerings (“STOs”), an alternative to ICOs whereby the tokens being sold to participants are of securities nature (commonly referred to as “Security Tokens”). STO has also introduced the cryptocurrency economy to other new business opportunities including

cryptocurrency exchanges that wish to provide trading services to these Security Tokens and technical issuance platforms. Such market trend initiated a range of new regulatory approaches and initiatives to promote fintech development from the SFC and several agencies, given that the Security Tokens would seemingly fall under the jurisdiction of the SFC as bestowed to them through the SFO, including the additional licensing conditions on licensed corporation and the expansion of the regulatory “sandboxes” (as discussed below) as initiated in the 2018 SFC Statement. Hong Kong now appears to take a more proactive approach in exploring the regulation over virtual assets, in particular Security Tokens.

Cryptocurrency regulation

As mentioned above, the HKMA and the SFC have recognised Bitcoins and other currencies like it as a “virtual commodity” (it is not clear if and how this extends to other Altcoins), which is a sub-category of “virtual assets” and Hong Kong has not created new legislation or regulations to define those terms. The SFC has not made further clarification on which tokens or coins would fall under the new asset class of “virtual asset” but has admitted that many virtual assets do not necessarily constitute “securities” or “futures contracts” for the purpose of the SFO (which the SFC has now specifically confirmed Bitcoins and Ether as examples), which may be referred to as “Non-SF Virtual Assets”.

Certain businesses which are common in the cryptocurrency economy are ordinarily regulated in Hong Kong, and thus a cryptocurrency company that wishes to participate in such market must abide by such specific legislation.

Hong Kong does not regulate private possession or transfer of cryptocurrencies between private individuals, on the assumption that the cryptocurrency in question was obtained and is transferred in good faith (cryptocurrencies are subject to anti-money laundering (“AML”) laws which are discussed below).

One of the most noteworthy regulated industries that is quite pervasive in the cryptocurrency economy is the ICO space. ICOs are campaigns where issuers sell blockchain-based tokens to potential participants in exchange for other cryptocurrencies such as Ether or Bitcoin. The purpose of conducting an ICO is to crowdsource funds for a specific project that the issuer aims to develop, and the tokens have certain “utility” within such project; therefore the tokens sold in ICOs are commonly referred to as “Utility Tokens”. One example is the OAX project (<https://www.oax.org/en>), which was considered the first ICO in Hong Kong. The conventional ICO follows the ERC-20 Ethereum standard and the sale is conducted through a web portal. Aside from the technical elements, the issuers also circulate several documents to the public during the ICO period such as the white paper (or even technical white paper) and the token sale agreement, if any.

Another type of campaign that is similar to ICOs is STOs, which has risen to attention in recent years. The issuance process of a STO is similar to an ICO save that the tokens being exchanged in return would be Security Tokens, i.e. it possesses the characteristics of equity, debt, structured products or collective investment scheme (the common types of securities under SFO), therefore would be subject to the provisions of the SFO. The offering of the Security Tokens would therefore need to be conducted in compliance with the SFO and in a similar manner as the offering of traditional securities products, including but not limited to the requirement of dealing through intermediaries that are licensed with the SFC and the requirement of publishing an offering memorandum (or “prospectus” depending on the type of offering being made or whether certain exemptions under the SFO have been relied on). As an industrial practice, the documents commonly found in an ICO, i.e. the White Paper, would also be published.

In general, Hong Kong does not prohibit the possession or trading of Non-SF Virtual Assets, as Bitcoins and currencies similar to it are considered to be virtual commodities and not electronic money, provided the cryptocurrencies are possessed and traded in good faith. There are other regulatory considerations depending on the use of cryptocurrencies, such as the running of ICO campaigns or trading Bitcoin futures contracts.

Sales and distribution of cryptocurrencies

As remarked in the paragraph above, the government has a duty to safeguard the free flow of capital as enshrined under Article 112 of the Hong Kong Basic Law. Trade controls and consumer protection are predominantly controlled by the CED, and the basic trading of cryptocurrencies is subject to oversight by CED. The applicable legislation and regulations on the trading of cryptocurrencies will depend on the actual features of each particular cryptocurrency; for example, some tokens commonly known as “ICO tokens” may actually be Security Tokens instead by nature, i.e. it takes the form of or possesses features that are common in other financial products such as shares, debts, loan notes, interests in a fund or securitisation of another asset or asset class, if not correctly structured. These tokens will therefore be regulated by the applicable legislation such as the SFO.

Trading of Bitcoin in Hong Kong is commonly done on cryptocurrency exchanges, on over-the-counter (“OTC”) desks and peer-to-peer (“P2P”) platforms with both consumers and institutional participants; depending on the nature of the transaction, different legislation will apply. In most business-to-consumer transactions conducted on exchanges and OTC desks, general consumer protection laws such as the Sales of Goods Ordinance (Cap. 26) and the Trade Descriptions Ordinance (Cap. 362) apply, with the former specifying the procedures and rights of parties in the transaction, and the latter setting out rules on the prevention of unfair trade practices. Business-to-business transactions are not covered *per se* by the above statutes which are mostly aimed at protecting individual consumers.

Certain commodity exchanges are prohibited from establishing in Hong Kong, under the Commodity Exchanges (Prohibition) Ordinance (Cap. 82) with the list of prohibited commodities being specified in the Schedule of the above Ordinance (“Schedule”), e.g. barley, cocoa, coffee, copper, cotton, gold, jute, lead, maize, oats, oil seeds and vegetable oils, platinum, rice, rubber, silver, soybeans, sugar, timber, tin, wheat, zinc, and frozen meat, poultry and fish. To date, cryptocurrency (or “virtual commodity”) has not been added to the Schedule, and therefore there are no statutory prohibitions on operating exchange in Hong Kong for trading of cryptocurrencies, which are classified as virtual commodities.

Cryptocurrency exchanges and OTC desks do also observe other legal requirements such as AML and counter-terrorist financing (“CFT”) and customer due diligence checks (further discussed below). There are certain cryptocurrencies that will be restricted in trading on the abovementioned platforms; the first type of restricted cryptocurrencies is Security Tokens.

In the 2019 SFC Statement, the SFC stated that Security Tokens are normally digital representations of ownership of assets (e.g. gold or real estate) or economic rights (e.g. a share of profits or revenue) utilising blockchain technology. The SFC considers that Security Tokens are likely to be “securities” as defined under the SFO and as such are subject to the securities laws of Hong Kong. Under Schedule 1 of the SFO, there are different categories of “securities”, mainly:

- *Shares* – shares are defined under the Companies Ordinance (Cap. 622) and in the common law relate to an equitable ownership interest of a company; such interest gives the shareholders certain rights, as stipulated in the company’s articles of association. A

cryptocurrency token can form a blockchain-based share certificate, if each token unit represents, *inter alia*, legal or beneficial ownership in the company, a right to vote in shareholders' meetings, and a right to receive dividend or some kind of distribution. Public offerings of such cryptocurrencies would be restricted on the basis that in Hong Kong, under the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32) ("CWUMPO"), a person shall not issue any form of application for shares in (or debentures) of a company to the public unless the form is issued with a prospectus which complies with the requirements under the same ordinance, unless one of the exemptions is applicable.

- *Debentures* – encompasses various debt-based instruments issued by a company. This category is quite broad as it is not necessary for a debenture to be expressly described as one; all that is required is that the instrument evidences a debt obligation by the company, whether or not the debt is charged against the company. Cryptocurrencies that share such features could be considered debentures and, as mentioned above under the CWUMPO, should be distributed subject to similar restrictions.
- *Structured products* – mainly include products and investment agreements such as equity-linked deposits or equity-linked investments (sometimes a hybrid of securities and regulated investment agreements). "Structured product" is defined under the SFO to instruments which return or amount due or the method of settlement is determined by the references to other price, value, level, securities, commodity, index, property, interest, rate, currency exchange rate or futures contracts. On a *prima facie* basis, this would appear to cover most derivatives products surrounding cryptocurrencies that are surfacing in the market over the last couple of years, but subject to further clarification from the SFC.
- *Regulated investment products* – as broadly defined in Schedule 1 of the SFO to include any contract that requires an investor to enter into with a profit calculated by changes in the value of any property. This would appear to be a catch-all product to cover most investment contracts whereby the investors are paying for the expectation of profit, in particular applicable to some cryptocurrencies projects where the elements of profits are heavily focused on, in contrast to focusing on the utility functions of the cryptocurrencies.
- *Collective investment schemes* ("CIS") – the provisions concerning CIS products aim to regulate investment products that are collective in nature; examples of such products include unit trusts and mutual funds. Unlike the definition of "shares" above, a CIS may form if the definition under Schedule 1 of the SFO, which includes four components, is satisfied:
 - there must be an "arrangement of property";
 - the participating persons do not have day-to-day control over the management of the property, whether or not they have the right to be consulted or to give directions in respect of such management;
 - the property is managed in whole or on behalf of the person operating the arrangements; and/or contributions and profits or income are pooled; and
 - the purpose or effect, or the pretended purpose or effect, is to enable the participating persons to receive: (a) profits, income or other returns represented to arise; or (b) payments from the acquisition or disposal of the property.

Any person or intermediary ("Intermediary") who carries out business involving Security Tokens in Hong Kong (or targeting Hong Kong investors) is required to be licensed or registered for regulated activities. Any person who markets and distributes Security Tokens (whether in Hong Kong or targeting Hong Kong investors) is required to be licensed or

registered for type 1 regulated activity (dealing in securities) under the SFO. Intermediaries being involved in STOs are reminded to comply with all existing legal and regulatory requirements in Hong Kong, in particular:

- *Professional investors only.* Under the current market, Security Tokens are normally offered to professional investors only. The 2019 SFC Statement confirms that Type 1 Intermediaries should only target clients who are professional investors as defined under the SFO.
- *Suitability obligations.* When the Intermediary makes recommendation or solicitation of a Security Token, it shall ensure the suitability of its recommendation or solicitation for that client is reasonable in all the circumstances having regard to information about the client of which the Intermediary is or should be aware through the exercise of due diligence.
- *Complex products.* The SFC considers that Security Tokens would be regarded as “complex product”, which is defined as “an investment product whose, terms, features and risks are not reasonably likely to be understood by a retail investor because of its complex structure”. Nevertheless, it is generally the Intermediary’s (in particular those that operates through an online platform) duty to assess whether a product is a “complex product” or not. If the Intermediary comes to the conclusion that any Security Token it intends to distribute is a “complex product”, it should adopt additional investor protection measures to better protect clients’ interests by ensuring that clients are well informed about the key nature, risks and features of such Security Token and such Security Token is suitable for them.
- *Product due diligence.* Intermediaries distributing Security Tokens should conduct proper due diligence for the purpose of developing an in-depth understanding of the STOs and also ascertaining the risk return profile of such STOs.
- *Information for clients.* In order to help clients make an informed investment decisions, Intermediaries should make clear and adequate disclosure of the material information relating to the STOs in an easily comprehensible manner in order to help clients making an informed investment decision, including but not limited to: providing clients with access to up-to-date STO offering documents and other information; providing clients with material information as soon as reasonably practicable to enable clients to appraise the position of their investments, etc. Intermediaries should also provide prominent and clear warning statements to clients prior to and reasonably proximate to the point of sale or advice.

Should there be any failure to comply with the legal and regulatory requirements during the distribution of STOs, the fitness and properness of the Intermediary may be affected and SFC disciplinary action may follow.

Furthermore, in compliance with the “Circular to Intermediaries on compliance with Notification Requirements” issued by the SFC on 1 June 2018, the SFC has confirmed that any service involving trading of crypto-assets would be considered a significant change in the nature of business of the Intermediary and would be subject to the notification requirements under the Securities and Futures (Licensing and Registration) (Information) Rules (the “Information Rules”), and the 2019 SFC Statement urges the Intermediary to notify the SFC should they wish to be engaged in cryptocurrency-related businesses.

Given the broad nature of the CIS definition (as discussed above), it could be argued that many ICO campaigns could fall within the parameters of the CIS definition, thus being a Security Token. If this is the case, the issuer may not make the ICO open to the public without prior authorisation from the SFC and be in compliance with the SFO as mentioned

above. In March 2018, the SFC halted the ICO operated by a company called Black Cell Technology Limited (“Black Cell”), which allowed token-holders to redeem their tokens into equity shares in Black Cell. The SFC has considered this arrangement to be a CIS under the circumstances. In the above case, Black Cell has undertaken not to proceed with the ICO. It is important to note that in light of the SFC’s numerous statements to date, the regulators are closely observing the ICO and broader cryptocurrency economy to ensure that the relevant securities legislation is complied with, thus cryptocurrency exchange must conduct sufficient legal due diligence to ensure the cryptocurrencies they allow on their marketplace are not considered “securities” otherwise they will also be subject to the provisions under SFO.

Aside from securities, other types of financial instrument markets have also developed in the cryptocurrency economy. Bitcoin-based derivatives products have enjoyed considerable popularity, trading on exchanges such as Bitmex. Bitcoin futures gained even more popularity in late 2017 when CBOE and CME started offering Bitcoin futures contracts. The SFC stated in its announcement on 11 December 2017 that any intermediary in Hong Kong that offers brokerage services for the above Bitcoin futures will be required to obtain the appropriate licences from the SFC (namely “Type 2” when dealing with such futures contracts, and “Type 5” when advising on such futures contracts).

In the broad sense, trading of cryptocurrencies is not restricted in Hong Kong so long as they are classified as “virtual commodities” (and not Security Tokens) and do not infringe on any applicable securities and futures legislation. Cryptocurrency exchanges are not subject to legislation that prohibits the operation of commodity exchanges (but are subject to the laws on commodity exchange as mentioned above).

Virtual asset funds (commonly known as crypto funds)

Along with the 2018 SFC Statement, the SFC issued an appendix titled “Regulatory Standards for Licensed Corporations Managing Virtual Asset Portfolios” (the “Regulatory Standards”) and a “Circular to intermediaries: Distribution of virtual asset funds” (the “Circular”), which focused on the SFC’s stance and the regulatory standards to be imposed on: (i) Intermediaries that are licensed to manage portfolios or intend to manage portfolios that invest in virtual assets (the “Type 9 Intermediaries”); and (ii) Intermediaries that are licensed to distribute funds or intend to distribute virtual asset funds in Hong Kong (the “Type 1 Intermediaries”).

Interestingly, the SFC has confirmed that, where a firm only manages a “portfolio” (which covers CISs and discretionary accounts in the form of an investment mandate or a pre-defined model portfolio) which invests solely in Non-SF Virtual Assets, it is not required to be licensed or registered for Type 9 regulated activities (asset management) (the “Type 9 Licence”), but where a firm manages a fund of funds (even with the underlying fund investing solely in the Non-SF Virtual Assets), the firm is required to be registered for Type 9 Licence (asset management).

Pursuant to the 2018 SFC Statement and the Regulatory Standards, the SFC has developed a set of principles-based standard terms and conditions which would be imposed as licensing conditions (the “VA Licensing Conditions”) on the Type 9 licensed intermediaries (the “Type 9 VA Licensed Intermediary”) which manage or plan to manage portfolios with: (i) a stated investment objective to invest in Virtual Assets; or (ii) an intention to invest 10% or more of the gross asset value (the “GAV”) of the portfolio (the “*De Minimus* Threshold”) in Virtual Assets (collectively, the “Virtual Asset Portfolio(s”).

The key VA Licensing Conditions to be imposed include but are not limited to (i) only professional investors are allowed, with proper risk disclosure, (ii) no less than HK\$3 million liquid capital, (iii) appropriate portfolio valuation principles must be adopted, (iv) an independent, experienced and capable auditor must be appointed, and (v) an appropriate custodial arrangement must be in place. In particular in relation to condition (ii), a Type 9 VA Intermediary which holds Non-SF Virtual Assets (which, strictly speaking, does not constitute “client assets” under the SFO) for portfolios under its management shall be required to maintain a required liquid capital of not less than HK\$3 million (or its variable required liquid capital, whichever is higher).

In addition, the SFC has also confirmed in the Regulatory Standards and the Circular that if a firm distributes a fund under its management that solely invests in Non-SF Virtual Assets in Hong Kong (i.e. the management of such fund’s portfolio does not require a Type 9 Licence), it is still required to be licensed or registered for Type 1 regulated activities (dealing in securities) (“Type 1 VA Licensed Intermediary”) and depending on whether it is authorised by the SFC, the Type 1 VA Licensed Intermediary is required to comply with certain requirements.

Such regulatory approach from the SFC has indicated its acceptance of virtual asset funds being distributed and managed in Hong Kong provided the requirements imposed are fulfilled. As a result, the Hong Kong market has seen a surge of Type 9 Intermediaries making application to the SFC to notify the SFC of its intention to change the nature of its business, in the view of providing services to virtual asset funds. Consequently, Hong Kong may be a good alternative jurisdiction for many fund managers to consider should they wish to launch virtual asset funds, in light of the increasing difficulties in other offshore jurisdictions when dealing with virtual assets.

Taxation

In general, there is no capital gains tax payable from the sale of financial instruments in Hong Kong. That being said, any Hong Kong-sourced income from frequent cryptocurrency trading in the ordinary course of business may be treated as income in case of individual clients, and profits in case of a corporation, and subject to income tax and profits tax, respectively, regardless of whether the trading is made in exclusive cryptocurrency or fiat-to-cryptocurrency exchanges. In March 2020, the Inland Revenue Department issued the Departmental Interpretation and Practice Note No. 39 (Revised) on profits tax regarding digital assets, which confirmed that:

- The profits tax treatment of digital tokens would depend on their nature and use, which can be broadly classified into three categories: (i) payment tokens; (ii) security tokens; and (iii) utility tokens.
- For ICO issuers, the tax treatment of the proceeds from an ICO generally follows from the attributes of the tokens that are issued, for example: (i) if the ICO tokens represent equity or ownership interests in the issuer, the ICO proceeds would be capital in nature since the ICO token holders would be given shareholders’ rights; and (ii) if the ICO tokens give a right to future benefits without any equity or ownership interests, such tokens would require the ICO issuer to supply a good or to perform a service for the token holder. The ICO proceeds would be more likely be viewed as a prepayment for future goods or services. The timing of revenue recognition would depend on the details of the ICO issuer’s performance obligations, determined in line with generally accepted accounting principles. As a result, subject to any specific exemptions provided, profits arising in or derived from Hong Kong from an ICO can be charged to profits tax.

- If digital assets are bought (e.g. through ICO or exchange platform) for long-term investment purposes, such digital assets are more likely to be considered “capital assets” (*cf.* trading stocks) and any profits from disposal of such capital assets would not be chargeable to profits tax. Whether the digital assets are capital assets or trading stock has to be considered on the basis of facts and circumstances, applying the existing tax principles like “badges of trade”.
- Hong Kong-sourced profits from cryptocurrency business activities are chargeable to profits tax. The broad guiding principle will be applied to determine the source of profits from cryptocurrency transactions (e.g. what were the person’s operations that produced the relevant profits and where those operations took place).
- If cryptocurrency is used for business transactions, they should be accrued based on the prevailing market value as of the date of transaction.
- If cryptocurrency has been received as employment income, the amount to be reported should be the market value of the cryptocurrency at the time of accrual.

Pursuant to a press release dated 3 April 2019, the government confirmed that the Inland Revenue Department does not maintain statistics specifically on tax payable by persons carrying on virtual asset-related activities and each case should be assessed on the basis of its own individual facts and circumstances. The Inland Revenue Department would also, if necessary, seek relevant information from other tax authorities through the exchange of information mechanism under tax treaties to assess the situation.

Money transmission laws and anti-money laundering requirements

Many jurisdictions have implemented stringent anti-money laundering and counter-terrorist financing (“AML/CTF”) laws and regulations, with the majority implementing recommendations set out by the Financial Action Task Force (“FATF”), an international inter-governmental organisation that aims to standardise AML/CTF systems around the world.

In Hong Kong, the principal AML/CTF legislation is the Anti Money Laundering and Counter Terrorist Financing Ordinance (Cap. 615) (“AMLO”) which applies to financial institutions (including HKMA-authorized institutions, i.e. banks, SFC-licensed corporations, licensed insurance companies, stored value facility issuers and money service operators) and “designated non-financial business and professions” (“DNFBP”) (professions such as being lawyers, public accountants, estate agents, and trust and company services agents), and also creates a licensing regime for money service operators, and trust and company services providers. Businesses that principally deal with cryptocurrencies such as exchanges and OTC desks are not directly subject to the provisions of AMLO, as such businesses do not fall within the definition of a financial institution or DNFBP unless the cryptocurrency business partially operates in a regulated business, for example, providing money services such as money changing and remittance services. Further to the rules set out in AMLO, each regulatory authority has formulated its own guidelines on dealing with AML/CTF issues.

As mentioned in the section on “Government attitude and definition” above, the regulatory authorities in Hong Kong have maintained a cautious approach to cryptocurrencies. In 2014, both the HKMA and the SFC issued circulars to their respective supervised institutions warning of the anonymous nature of cryptocurrency transactions and their inherent money-laundering and terrorist-financing risks. These statements came around the same time as the most noteworthy cryptocurrency money-laundering case stemming from the apprehension and conviction of Ross Ulbricht, the operator of the deep-web marketplace, “Silk Road”.

Both regulators have clearly indicated the requirement for increased vigilance when dealing with cryptocurrency business, including inquiring into the internal controls on AML/CTF policies and procedures of the cryptocurrency businesses. In light of these requirements, many cryptocurrency businesses voluntarily apply the customer due diligence measures set out in the Schedule 2 of AMLO as part of their AML/CFT policies.

While AMLO sets out specific guidelines applicable to financial institutions and DNFBPs, other businesses and individuals have a statutory duty to report any suspicious transactions under various criminal statutes, namely the Drug Tracking (Recovery of Proceeds) Ordinance (Cap. 405) (“DTRPO”), Organised and Serious Crimes Ordinance (Cap. 455) (“OSCO”), and the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) (“UNATMO”). Any suspected transactions involving money laundering, terrorist financing or receipts of crime must be reported to the JFIU by submitting a suspicious transaction report (“STR”); failure to file a STR is a criminal offence which is liable to a fine of HK\$50,000 and a three-month imprisonment. As highlighted above, many cryptocurrency businesses implement AML/CTF measures to comply with the relevant suspicious transaction reporting provisions under the DTRPO, OSCO and UNATMO, and also the likely requests from their banks in Hong Kong.

Promotion and testing

Various regulatory bodies in Hong Kong embrace the government’s plan to promote fintech and financial innovation in the city. Currently the HKMA, SFC and the Insurance Authority are operating “sandbox” programmes that allow innovative financial products to be tested in a limited regulatory environment.

The first regulatory sandbox was introduced by the HKMA on 6 September 2016 (the “HKMA Sandbox”). The HKMA Sandbox provides HKMA-authorised institutions (“AIs”), e.g. banks, to allow for live testing of financial technologies before their formal launch. AIs must set applicable boundaries to conduct the trials on the client base and must offer appropriate customer-protection measures to resolve customer losses. On 28 November 2017, the HKMA introduced the Fintech Supervisory Sandbox 2.0 Chatroom that allows AIs to receive supervisory feedback through emails, video conferences and face-to-face meetings from the HKMA’s Fintech Facilitation Office and Banking Department during the early stages when the new technological application is being contemplated by the AIs. As of July 2018, the HKMA reported that it had supervised four distributed technology projects; this means that banks in Hong Kong are actively looking at rolling out blockchain technologies as part of their services. One of the visible disadvantages of the HKMA sandbox is that it is only available to AIs or technology companies that are associated with an AI. Technology start-up companies who do not meet the above criteria are not permitted to access the HKMA sandbox.

The SFC sandbox was announced on 29 September 2017 (the “SFC Sandbox”). The objective of the SFC Sandbox is to allow firms to utilise innovative technologies and demonstrate a genuine commitment to carry out SFC-authorised activities through the use of financial technology that may increase the quality of products and services for investors in Hong Kong. The SFC Sandbox will be opened to qualified firms who are “fit and proper” and hold applicable SFC licences and comply with the licensing requirements such as Financial Resources Rules. The SFC will impose licensing conditions on firms in the SFC Sandbox, which can be removed upon the firms’ exit from the SFC Sandbox when the firm satisfies the requirements to operate outside of the SFC Sandbox. The guidelines from the SFC do not specify what technologies are permitted in the SFC Sandbox as they only require

a genuine commitment to use financial technology in carrying out regulated activity, i.e. a cryptocurrency-based service that falls within the preview of regulated activity. Similar to the HKMA Sandbox, access to the SFC Sandbox is also limited to firms that hold SFC licences or people who qualify for SFC licences, which may also limit the access to the SFC sandbox for start-up companies.

Along with the 2018 SFC Statement, the SFC issued an appendix titled “Conceptual Framework for the Potential Regulation of Virtual Asset Trading Platform Operators” (the “Conceptual Framework”), setting out the potential regulations over “virtual asset trading platform operators” (commonly known as the “cryptocurrency exchanges”) (the “Platform Operators”). The Conceptual Framework expanded the existing SFC Sandbox to cover the operation of cryptocurrency exchange (referred to as the Virtual Asset Trading Platform in the 2018 SFC Statement). If the SFC considers a Platform Operator is demonstrating commitment adhering to the high standards of the SFC, the Platform Operator may be placed in the SFC Sandbox where it will work closely with the SFC for the exploration of any prospect in the SFC granting licences to it, subject to licensing conditions. If, at the end of the initial stage of the SFC Sandbox, the SFC concludes that it is appropriate to grant a licence to and to regulate the Platform Operators, the SFC has indicated that it will consider granting a licence to a qualified Platform Operator and impose certain licensing conditions as set out in the Conceptual Framework.

Some of the key proposed licensing conditions include (i) restricting services to “professional investors” only who have passed the suitability test, (ii) AML/CFT requirements on customers, (iii) limitations on trading of ICO tokens within the initial 12 months, (iv) prevention of market manipulative and abusive activities, (v) ongoing reporting obligations, (vi) insurance requirements, and (vii) segregation and custody of customers’ money and virtual assets. In relation to “professional investors”, they should have shown sufficient knowledge in virtual assets (including the relevant associated risks) before being offered the trading services of virtual assets. The required level of knowledge in virtual assets is still subject to clarification. Platform Operators may also be subject to licensing principles where they must establish and disclose their virtual assets admission criteria, set up a committee responsible for decision-making to admitting virtual assets and also adopt a fee structure to avoid any potential, perceived or actual conflict of interest when receiving payment for admitting virtual assets. Another condition worthy of further mention relates to the insurance requirements. The Platform Operators may be required to take out an insurance policy for risks associated with the custody of virtual assets, such as theft or hacking. The SFC indicates that the insurance policy would be expected to provide full coverage for virtual assets held by a Platform Operator in hot storage and a substantial coverage (for instance, 95%) for those held in cold storage. There are currently very limited insurance options on the market and, even if available, given the relatively short history and the significant value fluctuation of virtual assets, it is possible that the insurance products would require a higher premium and thus increase the operation costs of the Platform Operators.

As a result of the 2018 SFC Statement, Hong Kong has witnessed a surge of Platform Operators expanding their business to cover the Hong Kong market with the hope of participating in the SFC Sandbox and eventually be granted a licence to trade Security Tokens. It has been reported that, on 21 August 2020, the SFC issued the first approval-in-principle for the application by OSL, a digital asset platform and member of BC Technology Group, to operate a virtual asset trading platform under a licence for Type 1 (dealing in securities) and Type 7 (automated trading service (“ATS”)) regulated activities and, once the conditions for final approval are satisfied, the licence will permit the operation of brokerage and ATS for digital assets, including security tokens.

Ownership and licensing requirements

Ownership of cryptocurrencies is currently not subject to any restrictions or regulations in Hong Kong, provided that they are obtained in good faith. Possession of cryptocurrencies may be illegal when their sources originate, amongst others, from computer crime, which under Hong Kong laws are proscribed in section 161 of the Crimes Ordinance (Cap. 200), and section 27A of the Telecommunications Ordinance (Cap. 171) and other applicable Hong Kong legislations including the DTRPO and the OSCO which establish offences for handling the proceeds of crime.

There are no requirements to date to obtain any licence to own or trade cryptocurrencies which are classified as “virtual commodities”. On the other hand, this statement is subject to exceptions when dealing with securities and futures involving cryptocurrencies, such as Bitcoin futures: a broker who wishes to offer such contract to their clients will require the appropriate SFC licences.

Mining

Mining is the process of creating new blocks on the blockchain; this process includes verifying transactions and collecting “block rewards” of cryptocurrencies. This type of activity is common to blockchain platforms that use the “proof-of-work” consensus algorithm, where the transaction is proved by the computing power used to process it. There are other consensus models such as “proof of stake”, where the block producers stake their cryptocurrencies to gain the rights to process the transaction.

Assuming that “mining” is considered mining of “proof of work”-based cryptocurrencies (such as Bitcoin) to date, there are no specific regulations governing mining of cryptocurrencies in Hong Kong. Moreover, to date no Hong Kong governmental body has issued any guidance that discourages, restricts or prohibits Bitcoin mining activities. Whether cryptocurrency mining is legally permitted in Hong Kong is subject to other regulations in Hong Kong under certain circumstances, will be discussed below.

Mining operations (especially for cryptocurrencies such as Bitcoin) can be highly industrialised operations, usually involving the use of hundreds of ASIC (application-specific integrated circuit) computers to mine cryptocurrencies. Such operations closely resemble large-scale data centre operations. Any regulations that apply to other similar applications such as data centres may also be applicable to cryptocurrency mining sites. In Hong Kong, data centre facilitation is overseen by the Office of the Government Chief Information Officer.

Businesses that intend to operate large-scale data centres should be aware of the relevant land-use rights stipulated under the laws of Hong Kong. Under the statutory Outline Zoning Plans (“OZP”) prepared by the Town Planning Board under the Town Planning Ordinance (“TPO”), such data centres belong to “Information Technology and Telecommunications Industries” for cryptocurrency mining purposes and would therefore require application for amendment to the OZP under section 12A of TPO. Apart from zoning permission, it should be noted that development of a site is subject to, *inter alia*: the terms and conditions of the land lease governing the site; the usage set out in the occupation permit; and the deed of mutual covenants, if any.

The operation of a data centre involves mechanical and electrical installations which may be subject to statutory requirements in Hong Kong. The key statute in question is the Buildings Energy Efficiency Ordinance (Cap. 610) and, in order to comply with the

ordinance, the owner or operator of a data centre in a prescribed building should engage a Registered Energy Assessor to certify that its building services installations have complied with the requirements under the above ordinance. The above rules would only be applicable to large-scale cryptocurrency mining operations and would not likely apply to domestic or small-scale mining operations.

Border restrictions and declaration

Prior to recent legislative changes, there were no statutory declaration requirements on the import and export of large quantities of money in Hong Kong as advised by FATF Recommendation 32. As of 16 July 2018, with the commencement of the Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance (Cap. 629) (“CMPCBNIO”), a person who physically imports or exports large amounts of currency or bearer-negotiable instruments (“CBNIs”) through the designated checkpoints stated in the CMPCBNIO must now disclose and declare such movement to CED. The disclosure threshold is set at HK\$120,000 (Schedule 4 of the CMPCBNIO).

The new CMPCBNIO is only applicable to CBNIs, which are defined as cash or negotiable instruments such as bearer cheques, promissory notes, bearer bonds, traveller’s cheques, money orders or postal orders. As Bitcoin has so far been classified by the HKMA as a “virtual commodity”, it should not fall within the definition of CBNI, but it is unclear how this would apply to other Altcoins. There would also be considerable difficulties in enforcing this provision, as CMPCBNIO requires the physical movement of CBNIs; thus to enforce the declaration requirements, the CED would have to prove that Bitcoins were physically moved across the border.

Reporting requirements

In Hong Kong, there is no requirement to report cryptocurrency transactions of any amount. Profits generated through cryptocurrency trading may be subject to declaration in a tax return under the applicable tax legislation, as discussed above. As cryptocurrencies are not defined as CBNIs, there is no obligation to declare them to CED when importing them to Hong Kong.

Estate planning and testamentary succession

In essence, any cryptocurrencies or cryptocurrency accounts would be treated as personal property and would fall into the estate of the deceased, which can be administered by the Executor named in the will of the deceased or an Administrator appointed by the Probate Court. The Executor or the Administrator could apply for a “Grant of Probate” or a “Letter of Administration” before he is allowed to handle the cryptocurrencies or exchange accounts.

Ordinary access to cryptocurrencies requires the user to have access to the private key to make transactions on the blockchain, and if the private key is lost then the cryptocurrencies are irrecoverable. Thus when conducting estate planning, arrangements should be made to preserve the private key beyond the death of its owner, such as recording the recovery seed and storing in a safe environment (i.e. a bank safe deposit box). Cryptocurrency exchange accounts may be accessed by the Executor or the Administrator in accordance with the procedures of each exchange; like with many internet-based services, this may require the Executor or the Administrator to submit the certificate of death, the Grant of Probate and/or the Letter of Administration to the exchange.

**Yu Pui Hang (Henry Yu)****Tel: +852 2115 9525 / Email: hyu@lylawoffice.com**

Mr. Yu is the founding partner of L&Y Law Office and Henry Yu & Associates. He obtained his Bachelor of Laws degree in England and is qualified as a solicitor in both England & Wales and Hong Kong.

Over recent years, Mr. Yu has developed a strong interest in the blockchain industry and his enthusiasm and insightful views have been affirmed widely by various professional bodies. Mr. Yu is a member of the Innotech Committee (a.k.a. the Technology Committee) of the Law Society of Hong Kong, and he has also been appointed as: Hon. Legal Advisor to the Hong Kong Federation of Innovation and Invention; Hon. Legal Advisor to the Institute of Financial Technologists of Asia; and Hon. Legal Advisor to the GHM-Greater Bay Area TECHFIN Association. From time to time, Mr. Yu represents the Bitcoin community at meetings with the Legislative Council Members, the HKMA and the FTSB.

L&Y Law Office / Henry Yu & Associates

Suite 806 / Suite 806A, 8/F, Tower Two, Lippo Center, 89 Queensway, Admiralty, Hong Kong

Tel: +852 2115 9525 / URL: www.lylawoffice.com

Ireland

Keith Waine, Karen Jennings & David Lawless
Dillon Eustace

Government attitude and definition

The Irish Government has been keen to demonstrate its support of the development and adoption of new technologies, including blockchain, as a way to encourage digitalisation and foster innovation. In a paper issued in December 2019 entitled “International Financial Services Strategy 2025” (**IFS2025**), the Irish Government stated its commitment to developing Ireland as a global leader in the financial services sector and announced measures aimed at demonstrating Ireland’s credentials as an EU centre of excellence for distributed ledger technology (**DLT**).

Since June 2018, the Industrial Development Authority (**IDA**), a semi-state body with a mandate to attract foreign direct investment into Ireland, has worked with the Irish Blockchain Expert Group on the “Blockchain Ireland” initiative. This forum is led by the IDA and seeks to enhance the blockchain industry in Ireland and to promote Ireland as a blockchain centre of excellence.

However, the Irish Government has so far been reticent in issuing firm guidance concerning its policy towards DLT and the treatment of virtual currencies from a legal and regulatory perspective.

In March 2018, the Department of Finance issued a discussion paper on Virtual Currencies and Blockchain Technology, with the general aim of describing the current environment, providing an overview of the global virtual currencies market and providing an overview of the potential risks and benefits of virtual currencies. On foot of this paper, an intra-departmental working group was established in 2018 in order to oversee developments in virtual currencies and blockchain technology and consider whether policy recommendations are required. No such policy recommendations have been issued to date.

The Central Bank of Ireland (**Central Bank**), as the authority responsible for the regulation of financial services in Ireland, has led the way by issuing consumer warnings on the risks of buying or investing in virtual currencies and initial coin offerings (**ICOs**).

In February 2018, consumers were warned by the Central Bank about the risks of buying or investing in “virtual currencies” and cryptocurrencies,¹ with the Central Bank highlighting risks such as extreme price volatility, the absence of regulation and the possibility of misleading information being provided by the currency issuer. The Central Bank emphasised that virtual currencies are a form of unregulated digital money that can be used as a means of payment, noting that they do not have legal tender status in Ireland, and are not guaranteed or regulated by the Central Bank.

Similarly, the Central Bank sought to alert consumers to the high risks associated with ICOs, such as vulnerability to fraud or illicit activities, lack of exit options, extreme price volatility,

inadequate information and exposure to flaws in the technology.² It has also indicated its support of the warnings published by the European Securities and Markets Authority (**ESMA**) concerning the risks of ICOs and crypto-assets³ whereby ESMA underlined the risks that the unregulated crypto-assets pose to investor protection and market integrity. ESMA identified the most significant risks as fraud, cyber-attacks, money laundering and market manipulation.

Crypto-assets (including cryptocurrencies) are not considered money or equivalent to fiat currency in Ireland and there are currently no cryptocurrencies that are backed by either the Irish Government or the Central Bank.

As discussed further below, Ireland is in the process of transposing the EU's Fifth Money Laundering Directive 2018/843/EU (**MLD5**) into Irish law, which extends anti-money laundering (**AML**) and countering the financing of terrorism (**CFT**) requirements to cover certain virtual currency exchanges and custodian wallet providers.

Cryptocurrency regulation

Although the Central Bank has issued warnings in relation to investment in crypto-assets, there is currently no blanket prohibition or ban on cryptocurrencies in Ireland. However, Ireland has not implemented a bespoke financial regulatory regime for cryptocurrencies and there are currently no plans to do so at a local level.

The question of whether and how crypto-assets are regulated under Irish law turns primarily on whether activities carried on in relation to those crypto-assets are regulated under existing legislation in Ireland which implements certain EU Single Market Directives, such as the Markets in Financial Instruments Directive 2014/65/EU (**MiFID**), the Electronic Money Directive 2009/110/EU (**E-Money Directive**) and the Payment Services Directive 2015/2366/EU (**PSD2**) and by various EU regulations, such as the Prospectus Regulation 2017/1129/EU, the Market Abuse Regulation 506/2014/EU and the Central Securities Depositories Regulation 909/2014/EU, which have direct force in Ireland.

The Central Bank has indicated its hesitancy towards issuing new domestic legislation to regulate crypto-assets and cryptocurrencies. In 2018, Gerry Cross, the Director of Policy and Risk at the Central Bank, indicated that:

“... it can be easy, when faced with a new and challenging issue or activity, for a regulator to say that A or B is very risky, or that X or Y can have harmful effects and to start in straightaway to consider how to restrict them, regulate them or even ban them. This is an approach that Andrea Enria, the Chair of the European Banking Authority has recently described as a “regulate and restrict approach”.

However it is important, in whatever we are looking at, that we take a considered approach; that we think about the potential benefits, including longer term benefits, as well as risks. We need to be clear and precise about what it is we are trying to achieve. We need to reflect on approaches to accomplishing those objectives which retain as much as possible of the potential benefits while addressing the harms, approaches that are in other words proportionate. We also need to think about the potential unforeseen consequence of regulation, including the desirability of giving a “regulatory imprimatur to the activity in question”.”⁴

As a result, the Central Bank has maintained a “wait and see” approach with regard to implementing domestic regulation, taking guidance from international regulators and most notably EU supervisory authorities.

On 19 December 2019, the European Commission launched a public consultation on the future EU framework for markets in crypto-assets. The consultation paper consists of three substantive parts, namely: (1) classification of crypto-assets; (2) crypto-assets that are not currently covered by EU legislation; and (3) crypto-assets that are currently covered by EU legislation. This consultation is the first step taken at EU level in preparing potential initiatives to specifically regulate crypto-assets in the EU.

In response to that consultation, the Central Bank issued a letter dated 30 April 2020 to the Directorate-General for Financial Stability, Financial Services and Capital Markets Union of the European Commission, in which the Central Bank advised that it is supportive of the initiative and that it welcomes the development of a more harmonised approach to crypto-assets. The Central Bank expressed the view that a harmonised taxonomy at EU level would facilitate a feature driven, case-by-case assessment by market participants and, as appropriate, National Competent Authorities, given the evolving nature of crypto-assets.

“Classic” cryptocurrencies (such as Bitcoin, Litecoin and Ether) that are not centrally issued and give no rights or entitlements to holders currently appear to fall outside of the scope of the existing regulatory regime in Ireland. This is on the basis that a pure, decentralised cryptocurrency is unlikely to be a transferable security and the Central Bank has emphasised that such cryptocurrencies are “*unregulated*”.⁵ However, an exception to this may apply in relation to the category of cryptocurrencies known as “*stablecoins*” – particularly, where these are pegged to, and are directly exchangeable on demand for, fiat currencies.

In the 2019 consultation, the European Commission sought to determine whether additional regulatory requirements should be imposed on both “*stablecoin*” and “*global stablecoin*” issuers when their coins are backed by real assets or funds. The Central Bank’s 2020 letter indicates that, in its view, “*the risks of ‘so called stablecoins’ for financial stability, monetary policy, consumer and investor protection, legal certainty and compliance with AML/CFT requirements are a key concern. Among the Central Bank of Ireland’s key concerns is that the issuing of currency should firmly remain under the remit of the relevant public authorities (i.e. central bank). Where the reach or other features of ‘so called stablecoin’ risk it being perceived as a currency, or operating as a quasi-currency, then it should be prohibited*”.

In the context of true utility tokens (i.e. tokens that can be redeemed for access to a specific product or service), the Central Bank indicated in its 2020 letter that “*it is not readily apparent to us that most utility tokens are, or should be, treated as financial products or that they should be regulated as such. However, we recognise that a utility token may, in substance be, or may become, a financial instrument (transferable security or e-money) and, in that case, it should be clear that it should fall within the regulatory perimeter. Cases where crypto assets start as, or claim to be, one thing but morph into the provision of financial services directly or indirectly should be closely monitored*”. In the absence of clear Irish or EU legislative guidance, a case-by-case basis analysis is required in order to determine if a utility token falls outside of the parameters of a transferable security for the purposes of MiFID.

In relation to security tokens (which may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits), the Central Bank expressed the view in its 2020 letter that it would be beneficial to have a harmonised taxonomy at EU level in relation to crypto-assets, including a harmonised definition of a security token as a transferable security. Hence, where these security tokens are closer to conventional debt instruments and equity instruments, the Central Bank has called for them to be “*consistently regulated, while allowing genuine utility tokens to remain outside the regulatory perimeter*”.⁶

Key to any future regulation of security tokens at an EU or Irish level will be the concepts of “financial instrument” and “transferable securities” under MiFID. A transferable security for the purposes of MiFID includes shares, bonds, derivatives and other instruments that give their holders similar rights or entitlements. The definition is not exhaustive and includes any security negotiable on the capital market with the exception of instruments of payment. It is clear that a security token may well be deemed to be a transferable security for the purposes of MiFID, which would mean that any entity providing an investment service or carrying on an investment activity with respect to the relevant crypto-asset will need to be authorised as an investment firm (and will need to comply with certain prudential and conduct of business requirements) unless it benefits from an exemption.

Unfortunately, in the absence of a specific regulatory regime at present, there is simply no “one size fits all” approach, and a case-by-case analysis must be adopted.

Furthermore, money transmissions laws and AML legislation may also apply to activities carried out in relation to cryptocurrencies (see below).

Sales regulation

Where a crypto-asset is deemed to involve an offer of transferable securities to the public, the requirements under the Prospectus Regulation (EU) 2017/1129/EU, as implemented into Irish law by the European Union (Prospectus) Regulations 2019 (together, the **Prospectus Regulations**), may apply.

The Prospectus Regulations impose requirements for an approved prospectus to have been made available to the public before: (a) transferable securities are offered to the public in the Ireland; or (b) a request is made for transferable securities to be admitted to a regulated market situated or operating in the EU. Unless an exemption applies (public offers made to certain qualified investors are, for example, exempt), a detailed prospectus containing prescribed content must be drawn up, approved by the Central Bank (or the appropriate EEA Member State financial regulator where Ireland is not the home state of the issuer of the transferable securities) and published before the relevant offer or request is made.

These requirements only apply to offers or requests relating to transferable securities, being anything that falls within the definition of transferable securities in MiFID (see above). In light of the Central Bank’s 2020 letter, the Prospectus Regulations would appear to be of primary concern for issuers of security tokens in Ireland.

In addition to the Prospectus Regulations, there are various e-commerce and consumer protection requirements in force in Ireland that are potentially applicable to sales of cryptocurrencies or crypto-assets or the offering of services related to cryptocurrencies or crypto-assets (such as exchange or wallet services) in or from Ireland.

Taxation

There are no specific rules for dealings in crypto-assets or cryptocurrencies; therefore, one has to have regard to the basic principles of Irish tax law. This means that determining the tax treatment of a cryptocurrency transaction requires an assessment of the activities and parties involved, Irish Revenue guidance, case law and relevant legislation. The Irish Revenue confirmed this in a publication issued in May 2018 (which was subsequently updated in April 2020).

Whether a supplier of services or goods receives payment of cryptocurrency *in lieu* of cash will not change how that supply is taxed in the hands of the supplier. There is no change

to when revenue is recognised or how taxable profits are calculated. Cryptocurrency is treated the same as any other foreign currency and as cryptocurrencies are not a functional currency for tax purposes, a company's accounts cannot be prepared in cryptocurrencies for tax purposes.

Whether dealing in cryptocurrencies will be treated as a trade of dealing or a capital transaction for taxation purposes will depend on the nature and level of activity of the dealer. Occasional investment in and disposals of cryptocurrencies would likely be treated as a capital receipt, currently taxed at 33%. Where there is significant and regular dealing, this could be considered to be trading, which for a company would be taxed at 12.5%, or the marginal higher rates for individuals. The actual tax position will depend on an analysis of the specifics of each transaction, and would need a case-by-case consideration, as is normal in determining whether a trading activity is being undertaken.

While cryptocurrencies are treated in the same manner as any other foreign currency, it is acknowledged by the Irish Revenue that the value of cryptocurrencies may vary between exchanges and that there may not always be a single exchange rate for cryptocurrencies. Therefore, a reasonable effort should be made to use an appropriate valuation for the transaction in question. In addition, where there is an underlying tax event involving the use of a cryptocurrency, there is a requirement in tax legislation for a record to be kept of the transaction including any record in respect of the cryptocurrency.

VAT is due in the normal way from suppliers of good and services sold in exchange for cryptocurrencies. Although the Court of Justice of the European Union and the Irish Revenue have adopted a different basis on which the actual transfer of cryptocurrencies are VAT-exempt, they nevertheless have ultimately come to the same result. Irish stamp duty should not arise, although as stamp duty is a tax on documents, the manner in which the transfer takes place would be worth monitoring to ensure that a stampable document has not been inadvertently created.

The territoriality aspect of cryptocurrencies is still an evolving area. Understanding the source or situs of cryptocurrencies may be of significance in determining if a person is subject to Irish tax (in particular non-Irish residents) in cross-border dealings. This is an area that is likely to evolve over time.

Money transmission laws

Money transmission services in Ireland may be subject to the local regulatory regime governing money transmission, but will more likely be subject to the European Communities (Payment Services) Regulations 2018 (which implement PSD2 into Irish law). The Payment Services Regulations focus on electronic means of payment rather than cash-only transactions or paper cheque-based transfers. These Regulations may be relevant where a crypto-asset could potentially be considered a payment instrument or if the issuer is operating a payment account. Core concepts of the Payment Services Regulations include "electronic cash" and the transfer of "funds". As neither of these concepts appears relevant in the case of classic cryptocurrencies, products or ancillary services related thereto, they would appear to fall outside the scope of the Payment Services Regulations.

In the case of crypto-assets other than classic cryptocurrencies or ancillary services, the Payment Services Regulations could be relevant. For example, the operator of a cryptocurrency platform who settles payments of fiat currency between the buyers and sellers of cryptocurrency could be viewed as being engaged in the regulated activity of money remittance/transmission.

In addition, the European Communities (Electronic Money) Regulations 2011, as amended (the **Irish E-Money Regulations**), which implement the E-Money Directive into Irish law, may be of relevance to certain types of crypto-assets. The Irish E-Money Regulations regulate the issuers of e-money. “Electronic money” is defined as “*electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer*”. Classic cryptocurrencies would not appear to involve “*a claim on the electronic money issuer*”. However, the European Banking Authority (**EBA**) has indicated that, in certain circumstances, a crypto-asset could qualify as “electronic money”,⁷ namely where the token is issued on the receipt of fiat currency and is pegged to, and directly exchangeable on demand for, such fiat currency (such as a stablecoin). We would expect the Central Bank to follow this view in Ireland.

Where a particular cryptocurrency qualifies as “electronic money”, then an Irish issuer will be required to be authorised under the Irish E-Money Regulations. Such an entity will therefore need to comply with ongoing financial regulatory requirements (some of which are likely to be problematical for certain crypto-assets) and would be subject to AML requirements.

Anti-money laundering requirements

MLD5 requires EU Member States to impose registration and AML requirements on fiat-to-cryptocurrency exchange platforms, as well as custodian wallet providers.

The General Scheme of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2019 (the **Irish Bill**), which seeks to implement MLD5 in Ireland, was published in January 2019 but has not yet been enacted. The deadline for the transposition of MLD5 into Irish law was 10 January 2020. On 14 May 2020, the European Commission sent a letter of formal notice to Ireland (along with seven other EU Member States and the UK) for having only partially transposed MLD5.

Under MLD5, “virtual currency exchange providers” are defined as meaning “providers engaged in exchange services between virtual currencies and fiat currencies”. This definition therefore excludes crypto-to-crypto exchanges. Under MLD5, a “custodian wallet provider” means “an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies”. The Irish Bill replicates these definitions.

In the 2019 public consultation on crypto-assets launched by the European Commission, the Commission indicated that it will be considering adding certain additional crypto-asset services to the EU AML/CFT legal framework obligations. In the Central Bank’s response letter of 30 April 2020, the Central Bank indicated that it agrees with the view that the five crypto-asset services⁸ specified in the Financial Action Task Force (**FATF**) definitions glossary should be covered by the EU AML/CFT legal framework obligations. It remains to be seen as to whether or not the European Commission will seek to extend the registration and AML requirements on these additional services in the future.

Promotion and testing

In April 2018, the Central Bank launched its Innovation Hub, designed to facilitate open and active engagement with the FinTech sector. The Central Bank has stated that:

“This was done with three aims in mind: firstly, to provide us with a way to engage more effectively with persons and entities engaged in fintech innovation, so that we as supervisors could gain an enhanced understanding of the developments underway

and likely to emerge. Secondly to enhance our discussions on regulatory aspects with innovators, for many of whom the world of financial regulation is an unaccustomed and potentially intimidating one. And thirdly, to help ensure that new financial firms emerging onto the market are well placed to comply with the requirements of financial regulation which is key to the continuing achievement of the consumer protection and financial stability outcomes that are at the heart of our mandate.”

However, to date, Ireland has not established a regulatory sandbox to allow firms to test innovative financial services propositions in the market with real consumers.

Ownership and licensing requirements

There are no specific prohibitions in Irish law on the ownership or control of crypto-assets. However, the nature and form of property rights that may exist in relation to crypto-assets under Irish law is currently untested.

As to licensing requirements, whether or not a person requires authorisation to perform their activities in relation to crypto-assets in Ireland will depend on a case-by-case analysis of the activities to be performed and the nature of the crypto-asset itself. It will also involve a case-by-case analysis of the various securities laws in Ireland arising under both EU and domestic legislation as detailed above under the headings “Cryptocurrency regulation”, “Sales regulation”, “Money transmission laws” and “Anti-money laundering requirements”. As in many jurisdictions, the regulatory environment in Ireland in relation to cryptocurrencies and their interaction with securities law is not yet settled.

Certain products, such as UCITS funds which are intended to be marketed to retail investors in the EU, are subject to specific restrictions on the type and diversity of assets they can hold, with such restrictions most likely excluding crypto-assets. However, there are no generally applicable restrictions in Ireland on investment managers holding crypto-assets for investment purposes, and as such, the regulatory position is unclear.

Certain crypto-assets (such as stablecoins) could potentially be categorised as an alternative investment fund in certain limited circumstances (such as where the value is pegged to the performance of a pool of underlying assets), giving rise to licensing requirements relating to the issue, operation and marketing of the fund and its service providers.

Mining

There are no specific restrictions on the mining of Bitcoin or other cryptocurrencies in Ireland. However, the Central Bank has been keen to highlight the potential negative environmental impacts of virtual currency mining.⁹ Concern regarding the environmental impact of virtual currency mining is especially relevant due to the recent focus of EU institutions on sustainable finance and the publication of the EU Commission’s Sustainable Finance Action Plan.

Border restrictions and declaration

There are no specific border restrictions or declarations that must be made on the ownership of cryptocurrencies in Ireland. Individuals carrying cash in excess of EUR 10,000 must declare this to the Revenue Commissioners on entering Ireland from a country outside the EU. However, as cryptocurrencies are not regarded as cash in Ireland, this requirement does not apply to cryptocurrencies.

Reporting requirements

Currently, there are no specific reporting requirements in place for crypto-assets in Ireland. However, any transactions should be monitored to ensure that they are compliant with AML and CFT procedures, particularly in light of the imminent implementation of MLD5 (see above).

Estate planning and testamentary succession

There is no explicit legislation in Ireland addressing the treatment of crypto-assets in the context of estate planning and testamentary succession. In principle, it is expected that any crypto-assets or crypto-assets accounts would be treated as personal property and would fall into the estate of the deceased, which can be administered by the executor (in the case of a will) or an administrator (in the case of intestacy).

* * *

Endnotes

1. <https://www.centralbank.ie/consumer-hub/consumer-notice/consumer-warning-on-virtual-currencies>.
2. <https://centralbank.ie/consumer-hub/consumer-notice/alert-on-initial-coin-offerings>.
3. ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019.
4. “Tomorrow’s yesterday: financial regulation and technological change” – speech given by Gerry Cross, Director of Policy and Risk at the Central Bank of Ireland at Joint Session: Banknotes/Identity High Meeting 2018.
5. <https://www.centralbank.ie/consumer-hub/consumer-notice/consumer-warning-on-virtual-currencies>.
6. Speech at Digital Finance in Europe by Gerry Cross, Director of Financial Regulation, Policy and Risk on 14 May 2020.
7. See Box 3 on page 13 of the EBA’s Report on Crypto Assets.
8. The five services are: (i) exchange between virtual assets and fiat currencies; (ii) exchange between one or more forms of virtual assets; (iii) transfer of virtual assets; (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and (v) participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.
9. Gerry Cross, Director of Policy and Risk, Central Bank, Speech at Joint Session: Banknotes/Identity High Meeting 20 March 2018.

**Keith Waine****Tel: +353 1 673 1822 / Email: keith.waine@dilloneustace.ie**

Keith is Head of the firm's Financial Regulation team and provides regulatory advice to international banks, investment firms, payments and e-money firms, and other financial services providers.

Keith advises on a range of regulatory matters, including authorisation processes, regulatory perimeter issues, MiFID, individual accountability and consumer protection. He has particular expertise in anti-money laundering (AML) compliance having previously been Head of Legal and Compliance with responsibility for AML at a full-service Irish bank.

Many of Keith's clients operate in the payments and e-money sector and he is currently advising a leading international crypto-assets and payments firm on their application for authorisation in Ireland.

Prior to joining Dillon Eustace, Keith spent 10 years working in industry in senior executive roles, including as Co-Founder and Chief Compliance Officer of a regulated alternative mortgage lender.

**Karen Jennings****Tel: +353 1 673 1720 / Email: karen.jennings@dilloneustace.ie**

Karen is a Senior Associate in the Financial Regulation team. Karen advises clients operating across a wide spectrum of financial services including asset and fund management, banking and payments, credit servicing and insurance. Karen provides advice on Irish authorisation and licensing issues and on regulatory and compliance matters affecting financial firms such as EMIR, AML/CTF requirements, confidential information and data protection requirements, outsourcing, business continuity and disaster recovery. Karen also advises clients on regulatory capital and corporate governance requirements.

**David Lawless****Tel: +353 1 673 1765 / Email: david.lawless@dilloneustace.ie**

David advises on all taxation aspects of financial services – including structured finance transactions, investment management, capital markets, real estate, private equity, banking, treasury and reinsurance. He established the Dillon Eustace tax practice in 2004 after joining the firm from PwC where he was a financial services tax partner since 1996. David has written and spoken extensively on tax topics and has participated in public/private tax committees in Ireland focused on making Ireland an attractive tax location. He is a member of the international and VAT tax committees of Irish Funds and the tax committees of the Alternative Investment Management Association, the Irish Debt Securities Association and the Law Society of Ireland.

Dillon Eustace

33 Sir John Rogerson's Quay, Dublin 2, D02 XK09, Ireland

Tel: +353 1 667 0022 / URL: www.dilloneustace.com

Italy

Massimo Donna & Lavinia Carmen Di Maria
Paradigma – Law & Strategy

Government attitude and definition

Boosting the adoption of digital technologies has been a priority for Italy's current government since it was sworn in. In particular, dedicated government schemes have been set up to fund digital startups as well as to promote and finance Artificial Intelligence as a means to innovate business practices. Such initiatives are especially aimed at industries that have traditionally been the cornerstone of the Italian business community, such as fashion, food, art and hospitality, but also specialist industrial sectors.

In this context, blockchain in general, and specifically its application in the field of cryptocurrencies, has been the centrepiece of the latest government efforts to promote innovation. Such efforts, though, have been partially stymied by a general resistance to adopt new payment systems in a country where cash is still the most common way to settle bills, which of course might facilitate tax evasion.

This resistance led the government to press ahead with its plan to turn Italy into a cashless society, by passing a law granting significant rebates to taxpayers who avoid paying in cash. Whilst such a measure is primarily aimed at fighting tax evasion, it will very likely make alternative payment methods, including cryptocurrencies, more popular with the general public.

The current Italian government has also passed legislation aimed at introducing a statutory definition of blockchain and Smart Contracts. In fact, by way of Law Decree no. 135 of 2019, Distributed Ledger Technologies (“DLTs”) have been defined as follows: “*Technologies and IT protocols which make use of a ledger which is shared, distributed, replicable, simultaneously accessible, with a decentralized architecture based on cryptography such that it allows for the recording, validation, updating, storing of verifiable data by each participant, non-alterable and non-modifiable.*” Of course, such an attempt to provide a statutory definition of DLTs has been received critically by a number of commentators, but the government has informally signalled that they would be happy to amend it if need be. In particular, critics have pointed out that the definition of DLT does not seem to include permissioned blockchain in which, depending on the applicable governance rules, administrators may be allowed to alter ledgers in determined circumstances.

Law Decree no. 135 of 2019 also provides a definition of Smart Contracts as a software programme that operates on DLTs and whose execution automatically binds two or more parties based on pre-determined arrangements between the same parties. Smart Contracts meet the written requisite, as required under Italian law in certain circumstances, by way of digital identification of the interested parties as per certain guidelines to be issued by *Agenzia per l'Italia Digitale*, a government agency charged with overseeing and promoting the adoption of innovative digital technology in Italy. However, such guidelines, which

were supposed to be published shortly after the passing of the Law Decree, have not yet been released, making a purely theoretical exercise of the lawmakers' definitory efforts.

The Italian legal system does not include a general definition of cryptocurrencies (although, as we will analyse later, sector-specific definitions have been introduced). Therefore, commentators have debated whether cryptocurrencies should be regarded as currency or goods from a legal standpoint. This is not just a theoretical issue, as it would have an immediate effect on a number of levels, including whether or not cryptocurrencies are suitable means of payment. After years of debate and uncertainty, consensus seems now to have been reached in the sense that cryptocurrencies are subject to the same legal regime as currencies that are not legal tender in Italy, e.g. outdated currencies, such as the Italian Lira which has been replaced by the Euro, and currencies of another country. Based on this theory, if a contractual payment is stipulated in a cryptocurrency, whilst the creditor is not entitled to payment in a currency other than that which was contractually agreed, the debtor can also make the payment in the currency having legal tender at the exchange rate of the date on which the payment obligation becomes due. Although to date no case law has confirmed such theory, it has been applied in an arbitration ruling (http://giustiziavivile.com/system/files/allegati/arbitro_unico_marcianise_-_14_aprile_2018_lodo_arbitrale.pdf).

As for the legal nature of cryptocurrencies, it should be pointed out that Italian Courts have not always aligned with the majority of commentators. In fact, the Italian Supreme Court has very recently regarded the online sale of bitcoin as the promotion of financial instruments, whilst the Court of Florence has labelled certain cryptocurrencies, which were held in deposit at an e-wallet and exchange outfit which later became insolvent, as “fungible goods” (Court of Florence, ruling no. 18 of 2019).

Also noteworthy is a ruling of the Court of Brescia of 2018 (Decree no. 7556 of 18 July 2018) in which the Court clarified the requirements that cryptoassets must meet to be eligible to be paid in as share capital of a *Società a Responsabilità Limitata* (broadly speaking, the Italian equivalent of a limited liability company). In fact, the Court confirmed that cryptocurrencies are eligible to be paid in as share capital on the condition that their value is determinable, typically as determined in broadly used exchanges. Hence, a request of certain shareholders to increase the company's share capital by paying in certain currencies that they had just created and negotiated on a very small, homemade crypto-exchange has been quashed by the Court. As for determining the legal nature of cryptocurrencies, the ruling of the Court of Brescia has not shed additional light, as it merely mentioned that under Italian law, both goods and services, in addition to cash, may be paid in as share capital.

Although in the political arena there have been talks of adopting “parallel cryptocurrencies”, nothing has ever come of it for fear that their implementation would impact the monetary policy that, as Italy is a Euro-area country, is the exclusive responsibility of the European Central Bank.

Cryptocurrency regulation

Although, as mentioned above, the Italian legal system does not include a general definition of cryptocurrencies, a statutory definition of “virtual currencies” has been included in Legislative Decree no. 90 of 2017 which has transposed in Italy the AML 4 Directive, as follows:

“[A] digital representation of value, which has not been issued or backed by a central bank or a public authority and which is not necessarily pegged to a legal tender, but which is used as a means of exchange for the purchase of goods or services or for investment purposes, and may be transferred, stored or negotiated electronically.”

This is certainly just an initial attempt to define such a complex phenomenon as cryptocurrencies and one in which virtual currencies are defined broadly, as the aim of the statute, including the definition, was to capture the wider possible range of digital currencies to prevent them from being used for money laundering and facilitating terrorism.

Thus, the use, storage and exchange of virtual currencies is not prohibited, although, as we will see later in more detail, providers of e-wallet and crypto-exchange services are subject to anti-money laundering (“AML”) regulation.

Cryptocurrencies as an investment

Initial Coin Offerings (“ICOs”) are not regulated in Italy. However, CONSOB, the Italian Financial Markets watchdog, has been trying to assess their possible impact on retail investors over the past few years.

In particular, CONSOB has been worrying about the ICOs’ white papers, whose content is not subject to statutory requirements, and is not assessed/verified by public authorities. As a result, it is left to the individual ability of retail – often unsophisticated – investors to assess the information contained in white papers. In addition, private enforcement is oftentimes difficult to carry out, since cryptocurrency issuers are difficult to pin down as they are incorporated in and/or operating out of exotic jurisdictions.

CONSOB has also been considering whether tokens typically issued in the context of an ICO are to be regarded as financial instruments and, therefore, subject to MiFID II requirements. In fact, having preliminarily noted that tokens are typically suitable to being negotiated on *ad hoc* blockchain platforms, CONSOB has pointed out that, depending on the characteristics of the tokens, they may or may not fall within the field of application of MiFID II. Indeed, whilst payment tokens are typically not covered by such legislation and investment/security tokens are (as they are similar to securities in scope and purpose), so-called utility tokens constitute a grey area which needs to be assessed on a case-by-case basis. For example, often utility tokens seem to only entitle the token-holder to receive a product or service in the future, but the token-holder may also intend the purchase of the token as an investment, in fact hoping that the future services or goods will appreciate over time, consequently causing an appreciation of the underlying “utility” token. In such a case, what at first may seem a utility token, on further analysis may reveal itself to be an investment token. Equally, some payment tokens may be purchased as a speculative investment instrument in light of their high volatility.

However, CONSOB soon realised that regulating ICOs in such a way based on an *ad hoc* analysis of the characteristics of the tokens to be issued does not guarantee the level of legal and regulatory certainty that is necessary to promote ICOs as a mainstream way to fund new entrepreneurial initiatives.

Also with this in mind, in 2019, CONSOB launched a public consultation on ICO regulation in Italy. In the consultation, CONSOB depicted a draft ICO regulation to be applied to cryptoassets that fall within the definition of “financial products” under the Finance Code (*Testo Unico della Finanza* or, in short, “TUF”) with the exclusion of those assets that are “financial instruments” under MiFID II. According to the draft project, token issuers may opt to offer cryptoassets through authorised platforms which, at least initially, may coincide with those offering equity-crowdfunding services under the relevant CONSOB regulation. In January 2020, CONSOB published the comments received – mostly from financial institutions, universities and law firms – which covered a number of issues, from the definitions of DLT and blockchain that in the consultation document appeared to

coincide, to the security measures that ICO platform managers should adopt. COVID-19 has generally slowed down the government's action outside the urgent measures to weather the pandemic, and CONSOB has not yet followed through on its plan to regulate ICOs. However, in our view, resuming action to bring to fruition all plans to regulate ICOs may be a key measure to ensure funding of tech startups and scaleups at a time where many commentators predict that banks will tighten up credit.

Sales regulation

In general, the lack of *ad hoc* regulation of cryptocurrencies is increasingly becoming a matter of concern as it is preventing widespread consumer and business adoption. A very recent ruling of the Italian Supreme Court (ruling no. 26897 of 25 September 2020) has added additional uncertainty, as it has sentenced certain individuals to harsh criminal punishment for selling bitcoins on the web for investment purposes. In fact, the Supreme Court found that given the methods and context within which bitcoins were promoted, they should have been regarded and authorised as financial instruments rather than payment systems.

Also, in 2018, CONSOB suspended an ICO which had been launched by a British company for breaching the statutes governing public offerings of financial products. In fact, after having ascertained that (i) the tokens offered through the ICO fell within the definition of financial products, and (ii) such tokens were offered to the general public in Italy, it proceeded to suspend the campaign.

Taxation

- (i) VAT. Unsurprisingly, the Italian tax authorities have stated that the activity carried out by cryptocurrency exchanges is exempt from VAT. This position reflects the finding of the Court of Justice of the European Union in its decision in *Skatteverket v David Hedqvist*, Case C-264/14.
- (ii) Corporate taxation. Equally unsurprisingly, the Italian tax authorities have stated that the profits deriving from cryptocurrency trading are relevant for the purposes of corporate income tax (IRES and IRAP) and must be included in the company's financial statements.
- (iii) Personal income tax. The profits generated by the trading of cryptoassets are regarded as those deriving from FOREX trading for personal tax purposes. In their annual tax return, individuals residing in Italy must specify whether they have any cryptocurrencies held in e-wallets, just as they have to declare if they have money held in foreign bank accounts.

Money transmission laws and anti-money laundering requirements

The AML 5 Directive has been implemented in Italy by way of Legislative Decree no. 125 of 2019. Even before transposing such directive into its legal system, Italy had imposed strict know-your-customer (“KYC”) and AML requirements upon both wallet service providers and exchanges.

Among other things, such cryptocurrency operators must enrol with an *ad hoc* register held as per Section 128 of the TUF.

Promotion and testing

Law 58 of 2019, among other things, has set up a FinTech Committee at the Ministry of Economy and Finance. The Committee is tasked with identifying specific objectives,

defining action plans and taking appropriate measures to facilitate techno-finance, also by way of cooperating with foreign partners, proposing statutory measures and acting as a liaison officer between industry players and the government.

The Committee is composed of a plethora of public authorities (e.g. the Ministry of Economy and Finance, the Bank of Italy, CONSOB, the Competition watchdog, the Data Protection Authority, *Agenzia per l'Italia Digitale* and the Italian Tax Authority) which will need to find a way to efficiently work together.

Law 58 also introduced regulatory sandboxes into our legal system, i.e. the possibility for innovative players operating in regulated sectors to benefit from a special regulatory regime to allow them to work with regulators to assess the impact of the introduction of their products or services in the relevant markets. Regulatory sandboxes will likely be applied mostly in the financial, banking and insurance sectors.

To this end, the Ministry of Economy and Finance was supposed to adopt specific regulations of an administrative nature to set out admission criteria to regulatory sandboxes and the specific working rules of such projects, whose duration cannot exceed 18 months. However, such measures have not been adopted as of the date of this writing.

As a parting remark, it should be pointed out that although the COVID-19 pandemic has shifted the government's attention towards more pressing issues than the implementation of the statutes and initiatives which were adopted lately, Italy has set the groundwork to possibly become one of the most crypto-friendly venues among the bigger European countries.

**Massimo Donna****Tel: +39 02 3655 2788 / Email: md@paradigma-law.com**

Massimo is head of the Technology Group at Paradigma – Law & Strategy. He advises clients on a broad range of technology and complex commercial matters. Massimo also advises clients on employment tech matters. Massimo was educated in Italy and Spain, trained in Italy and New York City and practised law as a foreign lawyer in London. Massimo also served as a senior in-house lawyer at various multinational tech companies. His mother tongues are Italian and English and he is also fluent in Spanish and French. Massimo routinely lectures on a range of technology law matters.

**Lavinia Carmen Di Maria****Tel: +39 02 3655 2788 / Email: ldimaria@paradigma-law.com**

Lavinia is an associate at Paradigma – Law & Strategy, where her practice focuses on complex IT contracts, Blockchain and Artificial Intelligence.

Paradigma – Law & Strategy

Piazza Luigi Vittorio Bertarelli 1, 20122 Milan, Italy
Tel: +39 02 3655 2788 / URL: www.paradigma-law.com

Japan

Taro Awataguchi & Takeshi Nagase
Anderson Mōri & Tomotsune

Government attitude and definition

General overview

With the steep rise of the price of Bitcoin and the increasing enthusiasm for initial coin offerings (“**ICO**”), the Japanese Crypto Asset market has seen explosive growth since 2018. In fact, Japan was the first country in the world to have enacted a law defining “Crypto Asset” as a legal term, and requires an entity to register as a Crypto Asset Exchange Service Provider (“**Exchange Provider**”) in order to provide Crypto Asset Exchange Services (“**Exchange Services**”) to residents in Japan. The definition of these terms will be discussed in detail in the section below entitled “**Cryptocurrency regulation**”.

The purpose of the above legislation is to: (i) protect customers of Exchange Providers; and (ii) combat money laundering and the financing of terrorism (“**AML/CFT**”).

The need for the above legislation can be traced to recent developments in the Japanese market. One such development is the civil rehabilitation, in February 2014, of MTGOX Co., Ltd., a Japanese company that provided convertible Exchange Services between Crypto Assets and fiat currencies, which was the world’s largest Crypto Asset exchange at that time. This case highlighted the urgent need for regulatory protection of Crypto Asset exchange customers.

In addition, following the Leaders’ Declaration at the G7 Elmau Summit, the Financial Action Task Force published the “Guidance for a Risk-based Approach to Virtual Currencies” in June 2015, which recommended that Virtual Currency exchanges be registered and/or licensed, and that they comply with regulations on money laundering and terrorist financing, including customer identification obligations.

Given these circumstances, a bill to amend the Payment Services Act (“**PSA**”) and the Act on Prevention of Transfer of Criminal Proceeds (“**APTCP**”) was submitted to the Japanese Diet on March 4, 2016, and was passed on May 25, 2016. The amended laws came into force on April 1, 2017.

Recent developments

In January 2018, Coincheck, Inc., one of the largest Crypto Asset exchanges in Japan, announced that it had lost approximately US\$530 million worth of cryptocurrencies through a hacking attack on its systems. In addition, it has also become apparent that Crypto Assets are being increasingly used for speculative reasons, rather than as a means of settlement.

This situation eventually led to the revision of certain pieces of legislation governing Crypto Assets, including the PSA and the Financial Instruments and Exchange Act (“**FIEA**”), etc. These revisions to the PSA (“**PSA Revisions**”) and the FIEA (“**FIEA Revisions**”), which

were intended to strengthen the regulatory framework surrounding Crypto Assets, came into force as of May 1, 2020.

The following is a summary of the key revisions.

- **PSA Revisions**
 - (a) Revision of the term “Virtual Currency” to “Crypto Asset”.
 - (b) Enhancement of regulation of Crypto Asset Custody Services.
 - (c) Tightening of regulations governing Exchange Services.
- **FIEA Revisions**
 - (a) Establishment of Electronically Recorded Transferable Rights (“**ERTRs**”) and regulations applicable thereto.
 - (b) Introduction of regulations governing Crypto Asset Derivative Transactions.
 - (c) Introduction of regulations governing unfair acts in Crypto Asset or Crypto Asset Derivative Transactions.

Central bank’s attitude toward cryptocurrencies

Under Japanese law, Crypto Asset is neither treated as “money” nor equated with fiat currency. No Crypto Asset is supported by the Japanese government or the central bank of Japan (the Bank of Japan, “**BOJ**”).

With that said, it should be noted that on July 2, 2020, the BOJ released a report entitled “Technological Challenges in Having Central Bank Digital Currencies Function as Cash Equivalents”, summarising the technical issues involved in getting central bank digital currencies to function as cash equivalents. In the report, the BOJ also mentioned that it may, through feasibility studies, verify the possibility of using central bank digital currencies as cash equivalents.

Cryptocurrency regulation

Under Japanese law, “Crypto Asset” is not listed as a type of “Security” as defined in the FIEA (please note, however, that a certain type of token may be subject to the regulation of the Act, as discussed later in the below section entitled “**Sales regulation**”). The PSA defines “Crypto Asset”, and requires a person who provides Exchange Services to be registered with the Financial Services Agency of Japan (the “**FSA**”). A person conducting Exchange Services without registration will be subject to criminal proceedings and punishment.

Therefore, the respective definitions of Crypto Asset and Exchange Services are of crucial importance.

Definition of Crypto Asset

The term “Crypto Asset” is defined in the PSA as:

- (i) proprietary value that may be used to pay an unspecified person the price of any goods purchased or borrowed or any services provided and which may be sold to or purchased from an unspecified person (limited to that recorded on electronic devices or other objects by electronic means and excluding Japanese and other foreign currencies and Currency Denominated Assets; the same applies in the following item) and that may be transferred using an electronic data processing system; or
- (ii) proprietary value that may be exchanged reciprocally for proprietary value specified in the preceding item with an unspecified person and that may be transferred using an electronic data processing system.

Though the definition is complicated, in short, a cryptocurrency that is usable as a payment method to an unspecified person and not denominated in a fiat currency falls under the definition of Crypto Asset.

“Currency Denominated Assets” means any assets that are denominated in Japanese or other foreign currency and do not fall under the definition of Crypto Asset. For example, prepaid e-money cards usually fall under Currency Denominated Assets. If a coin issued by a bank is guaranteed to have a certain value of a fiat currency, such a coin will likely be treated as a Currency Denominated Asset rather than a Crypto Asset. Please note that, under Article 2, Paragraph 5 of the revised PSA amending the term “Virtual Currency” to “Crypto Asset”, the existing definition of “Virtual Currency” will remain unchanged. Accordingly, it is generally understood that the change in reference from “Virtual Currency” to “Crypto Asset” will result in no substantive change to the legal interpretation of the term. Therefore, please note that, hereafter, when we refer to the relevant provisions under the PSA Revisions, we use the term “Crypto Asset” instead of “Virtual Currency” for the purposes of this chapter.

Definition of Exchange Services

Under the PSA, the term “Crypto Asset Exchange Services” means any of the following acts carried out as a business:

- (a) sale or purchase of Crypto Assets, or the exchange of a Crypto Asset for another Crypto Asset;
- (b) intermediating, brokering or acting as an agent in respect of the activities listed in item (a);
- (c) management of customers’ money in connection with the activities listed in items (a) and (b); or
- (d) management of customers’ Crypto Assets for the benefit of another person.

It should be noted that the PSA Revisions designates (d) “management of customers’ Crypto Assets for the benefit of another person” as a type of Exchange Service. Consequently, management of Crypto Assets without the sale and purchase thereof (“**Crypto Asset Custody Services**”) is now included in the scope of Exchange Services. Therefore, a person engaging in Crypto Asset Custody Services needs to undergo registration as an Exchange Provider. In this context, the FSA Administration Guidelines (Guidelines on Crypto Assets) describes the “management of customers’ Crypto Assets for the benefit of another person” as follows: “[A]lthough whether or not each service constitutes the management of Crypto Assets should be determined based on its actual circumstances, a service constitutes the management of Crypto Assets if a service provider is in a position in which it may transfer its users’ Crypto Assets (for example, if such service provider owns a private key with which it may transfer users’ Crypto Assets solely or jointly with its related parties, without the users’ involvement).” Accordingly, it is understood that if a service provider merely provides its users with a Crypto Asset wallet application (i.e., a non-custodial wallet) and private keys are managed by the users themselves, such a service would not constitute a Crypto Asset Custody Service.

Registration process for the Exchange Provider

The applicant must be (i) a stock company (*kabushiki-kaisha*), or (ii) a Foreign Exchange Provider which has an office(s) and representative in Japan. Accordingly, any foreign entity wishing to register as an Exchange Provider must establish either a subsidiary (in the form of *kabushiki-kaisha*) or a branch in Japan.

In addition, the applicant must have: (a) a sufficient financial basis (minimum capital amount of JPY 10 million and positive minimum net assets); (b) a satisfactory organisational structure and certain systems to conduct the Exchange Service appropriately and properly; and (c) certain systems to ensure compliance with relevant laws and regulations.

The applicant must submit a registration application containing, among others: (i) its trade name and address; (ii) the amount of its capital; (iii) the names of its director(s); (iv) the

names of the Crypto Assets it will handle; (v) the contents of and the means by which it will provide its Exchange Services; (vi) the name(s) of outsourcee(s) (if any) and the address(es) thereof; and (vii) the method by which the management of its users' Crypto Assets will be segregated from the management of its own Crypto Assets.

The registration application must be accompanied by documents including: (i) a document pledging that there are no circumstances constituting grounds for refusal of registration; (ii) an extract of the certificate of residence of the applicant's directors, etc.; (iii) a résumé of the applicant's directors, etc.; (iv) a list of the applicant's shareholders; (v) the applicant's financial documents; (vi) documents containing particulars regarding the establishment of a system for ensuring the proper, secure provision/performance of Exchange Services by the applicants; (vii) an organisational chart in respect of the applicant; (viii) the applicant's internal rules; and (ix) a form of the contract to be entered into with users.

During the registration process, the FSA will request for applicants to complete a checklist consisting of more than 400 questions, in order to confirm that the applicants have established systems to properly and securely perform the Exchange Service. In addition, the FSA will separately prepare a detailed progress chart to confirm the checking process. The registration process essentially serves as a due diligence exercise by the FSA, by which the FSA will determine whether to approve an applicant's registration. "Registration", if granted, will be akin to the issuance of a "licence" to the applicant.

Upon registration, the applicant's name will be added to the registry of Exchange Providers, which is publicly available.

Principal regulation on Exchange Providers

An Exchange Provider must: (i) take measures necessary to ensure safe management of information; (ii) provide information to users such as the content of transactions, an outline of each Crypto Asset handled by the provider, fees, the amount of cash or Crypto Assets that the provider has received from the user, the date of receipt, transaction records, etc.; (iii) take measures necessary for the protection of users and proper performance of its services; (iv) segregate users' property from its own property (with respect to cash, bank deposit or trust; with respect to Crypto Assets, clear distinction in a manner such that users' Crypto Assets are immediately identifiable), and regularly undergo an audit of the status of such segregated management by a certified public accountant or audit firm; and (v) establish an internal management system to make fair and appropriate responses to customer complaints and take measures to resolve any disputes through financial alternative dispute resolution proceedings.

Additional regulations applicable to Exchange Providers under the PSA Revisions

The PSA Revisions propose the following changes to the current regulatory system governing Exchange Providers in order to enhance the protection of users and to clarify the rules relating to Exchange Providers:

- (i) expansion of the grounds upon which applications for registration as an Exchange Provider may be rejected;
- (ii) introduction of a system of advance notification for any proposed amendment to certain matters in respect of the relevant Crypto Asset, such as the name thereof;
- (iii) introduction of regulations governing advertisement and solicitation in respect of Exchange Services;
- (iv) introduction of disclosure requirements where Crypto Assets are exchanged (or where certain similar transactions are undertaken) via the grant of credit to users;

- (v) enhancement of the obligation on Exchange Providers to preserve users' assets; and
- (vi) grant of rights to users to enable their receipt of preferential payments when claiming for the return of Crypto Assets.

However, with respect to (v) "enhancement of the obligation on Exchange Providers to preserve users' assets" above, under the PSA Revisions, an Exchange Provider is required to both manage the money of users separately from its own money, and to entrust users' money to a trust company or other similar entity that will act as trustee over users' money, in accordance with the provisions of the relevant Cabinet Office Ordinance.

In addition, the PSA Revisions require an Exchange Provider to manage users' Crypto Assets separately from other users' Crypto Assets in such manner as is specified in the relevant Cabinet Office Ordinance, in order to enhance the protection of users. The relevant Cabinet Office Ordinance requires an Exchange Provider to manage the Crypto Assets of users (other than Crypto Assets required for the smooth performance of Exchange Services) through highly reliable mechanisms, such as cold wallets.

Further, pursuant to the PSA Revisions, an Exchange Provider is required to (i) hold, for its own account, Crypto Assets of the same kind and quantity as the users' Crypto Assets that are subject to "requirements specified by the relevant Cabinet Office Ordinance as being necessary for ensuring users' convenience and the smooth performance of Crypto Asset exchange services" ("**Performance Assurance Crypto Assets**"), and (ii) manage Performance Assurance Crypto Assets separately from its own Crypto Assets (other than Performance Assurance Crypto Assets). In other words, when an Exchange Provider manages its users' Crypto Assets in hot wallets, the Exchange Provider would likely be required to (i) hold its own Crypto Assets of the same kind and quantity as the users' Crypto Assets that are managed in hot wallets, and (ii) manage Performance Assurance Crypto Assets in cold wallets separately from its own Crypto Assets (other than Performance Assurance Crypto Assets).

Sales regulation

Overview

Cryptocurrencies (including Crypto Assets) do not fall within the definition of "Securities" under the FIEA, and the sale of Crypto Assets or tokens (including ICO) are not specifically or directly regulated by the FIEA (although a certain type of token may be subject to the FIEA, as discussed below).

There are various types of tokens issued by way of ICO, and Japanese regulations applicable to ICOs vary according to the respective schemes.

Main types of tokens and applicable regulations

1. *Crypto Asset type*

If the token falls under the definition of Crypto Asset, the Crypto Asset regulation under the PSA is applicable. In accordance with the prevalent current practice, (i) if the tokens issued via ICO are already dealt with by Japanese or foreign exchanges, such tokens would be considered to fall within the definition of Crypto Asset under the PSA based on the rationale that exchange markets for such tokens must already be in existence, and (ii) even if certain tokens are not yet dealt with by Japanese or foreign exchanges, in a case where the token issuer does not give substantial restrictions prohibiting such tokens from being exchanged with Japanese or foreign fiat currencies or Crypto Assets, such tokens would likely fall within the definition of Crypto Asset under the PSA.

In addition, the Japan Virtual and Crypto Assets Exchange Association (“JVCEA”), which is a self-regulatory organisation established under the PSA, published self-regulatory rules and guidelines regarding ICOs for Crypto Asset-type tokens, entitled “Rules for Selling New Crypto Assets” (“ICO Rules”). According to the ICO Rules, there are two types of ICO, which can be described as follows: (i) an Exchange Provider issues new tokens and sells such tokens by itself; or (ii) a token issuer delegates Exchange Providers to sell the newly issued tokens. Generally speaking, the ICO Rules stipulate the following requirements for each type of ICO:

- (i) maintenance of a structure for review of a targeted business which raises funds via ICO;
- (ii) information disclosure of the token, the token issuer’s purpose for the funds, or the like;
- (iii) segregated management of funds (both fiat and Crypto Assets) raised by ICO;
- (iv) proper account processing and financial disclosure of funds raised by ICO;
- (v) safety assurance of the newly issued token, its blockchain, smart contract, wallet tool, and the like; and
- (vi) proper valuation of newly issued tokens.

2. *Securities (equity interest in an investment fund) type*

The FIEA Revisions introduced the concept of ERTRs, which clarify the scope of tokens governed by the FIEA. The concept of ERTRs relates to the rights set forth in Article 2, Paragraph 2 of the FIEA that are represented by proprietary value that is transferable by means of an electronic data processing system (but limited only to proprietary values recorded in electronic devices or otherwise by electronic means), excluding those rights specified in the relevant Cabinet Office Ordinance in light of their negotiability and other factors. Although Article 2, Paragraph 2 of the FIEA refers to rights of various kinds, tokens issued in “security token offerings” (“STOs”) are understood to constitute, in principle, “collective investment scheme interests” (“CISIs”) under the FIEA. CISIs are deemed to have been formed when the following three requirements are met: (i) investors (i.e., rights holders) invest or contribute cash or other assets to a business; (ii) the cash or other assets contributed by investors are invested in the business; and (iii) investors have the right to receive dividends of profits or assets generated from investments in the business. Tokens issued under STOs would constitute ERTRs if the three requirements above are satisfied.

To put it simply, rights treated as “Paragraph 2 Securities” (i.e., rights that are deemed as securities pursuant to Article 2, Paragraph 2 of the FIEA) and represented by negotiable digital tokens will be treated as Paragraph 1 Securities unless they fall under an exemption. As a result of the application of disclosure requirements to ERTRs, issuers of ERTRs are in principle required, upon making a public offering or secondary distribution, to file a securities registration statement and issue a prospectus. Any person who causes other persons to acquire ERTRs or who sells ERTRs to other persons through a public offering or secondary distribution must deliver a prospectus to such other persons in advance or at the same time.

As ERTRs are expected to constitute Paragraph 1 Securities, registration as a Type I Financial Instruments Business Operator will be required for the purposes of selling, purchasing or handling the public offering of ERTRs in the course of a business. In addition, any ERTR issuer who solicits acquisition of such ERTR (i.e., undertaking an STO), will be required to undergo registration as a Type II Financial Instruments Business Operator, unless such issuer qualifies as a specially permitted business for qualified institutional investors.

3. *Prepaid card type*

If the tokens are similar in nature to prepaid cards and can be used as consideration for goods or services provided by token issuers, they may be regarded as “Prepaid Payment Instruments” (*maebarai-shiki-shiharai-shudan*), which are subject to the relevant regulations of the PSA (in which case the regulations in respect of Crypto Assets in the same Act would not be applicable).

Introduction to regulations governing Crypto Asset Derivative Transactions

The FIEA Revisions regulate Crypto Asset Derivatives Transactions by establishing certain regulations in respect of Crypto Asset Derivatives Transactions, in order to protect users and ensure that such transactions are conducted appropriately. Specifically, for the purposes of subjecting derivatives transactions involving “Financial Instruments” or “Financial Indicators” to certain entry regulations and rules of conduct issued under the FIEA, the FIEA Revisions have included “Crypto Assets” and “standardized instruments created by a Financial Instruments Exchange for the purposes of facilitating Market Transactions of Derivatives by standardizing interest rates, maturity periods and/or other conditions of (Crypto Assets)” in the definition of “Financial Instruments”. Further, the FIEA Revisions have incorporated the prices, interest rates, etc. of Crypto Assets into the definition of “Financial Indicators”.

Since Crypto Assets are included in the definition of Financial Instruments, the conduct of Over-the-Counter (“OTC”) Derivatives Transactions related to Crypto Assets or related intermediary (*baikai*) or brokerage (*toritsugi*) activities will also constitute Type I Financial Instruments Business. Accordingly, business operators engaging in these transactions will need to undergo registration as Financial Instruments Business Operators in the same way as business operators engaging in foreign exchange margin trading.

Any entity that intends to be a Financial Instruments Business Operator engaging in Type I Financial Instruments Business is required to meet certain asset requirements, including having:

- (i) a stated capital of at least JPY50 million;
- (ii) net assets of at least JPY50 million; and
- (iii) a capital-to-risk ratio of at least 120%.

It should be noted that, traditionally, the registration requirements under the FIEA are not applicable to non-securities-related Derivative Transaction services provided to certain professional customers. However, the registration requirements will be applicable to Crypto Asset Derivatives Transactions, regardless of the type of customers involved, in light of the high-risk nature of Crypto Asset Derivatives Transactions. However, Foreign Crypto Asset Derivative Business Operators (i.e., companies that engage in Crypto Asset Derivatives Transactions in the course of a business in a foreign country, under applicable foreign laws and regulations) conducting OTC Crypto Asset Derivatives Transactions with certain professional entities in Japan will be excluded from the registration requirements in respect of the Financial Instruments Business Operators. Such professional entities are:

- (i) the government of Japan or the BOJ;
- (ii) Financial Instruments Business Operators and financial institutions that engage in OTC Crypto Asset Derivative Transactions in the course of a business;
- (iii) financial institutions, trust companies or foreign trust companies (provided they conduct OTC Crypto Asset Derivative Transactions only for investment purposes or on the account of trustors under trust agreements); and

- (iv) Financial Instruments Business Operators who engage in investment management business (provided that such entities engage in activities related to investment management business).

Introduction to regulations governing unfair acts in Crypto Asset or Crypto Asset Derivative Transactions

The FIEA Revisions contain the following prohibitions against unfair acts (the conduct of which is punishable by penalties) in respect of Crypto Asset spot transactions and Crypto Asset Derivatives Transactions, regardless of the violating party:

- (a) prohibition of wrongful acts;
- (b) prohibition on dissemination of rumours, usage of fraudulent means, assault or intimidation; and
- (c) prohibition on market manipulation.

These prohibitions are intended to enhance protection of users and to prevent unjust enrichment. However, insider trading is not regulated under the FIEA Revisions at this moment in time, due to difficulties in formulating a clear concept of Crypto Asset issuers, as well as the general inherent difficulties associated with the identification of undisclosed material facts.

Taxation

One of the most important issues in Japanese taxation of cryptocurrencies has been the treatment of consumption tax. Under Japanese tax law, sale of Crypto Assets has been subject to consumption tax in cases where the office of the transferor is located in Japan. However, the relevant tax law was amended in 2017. Accordingly, if the sold cryptocurrency can be considered a Crypto Asset (such as Bitcoin) under the PSA, consumption tax will not be imposed. The National Tax Agency of Japan also announced that gains realised by the sale or use of Crypto Assets shall be treated as “miscellaneous income” (*zatsu-shotoku*) where the taxpayer is unable to utilise losses elsewhere to offset gains realised by the sale or use of Crypto Assets. Furthermore, inheritance tax will be imposed upon the estate of a deceased person in respect of Crypto Assets that were held by such person.

Money transmission laws and anti-money laundering requirements

Money transmission

Under Japanese law, only licensed banks or fund transfer business operators are permitted to engage in the business of money remittance transactions. Money remittance transactions means, according to Supreme Court precedent, “to undertake the task of transferring funds requested by customers utilising the systems of fund transfer without transporting cash between distant parties, and/or to carry out such task”. Technically speaking, Crypto Asset does not fall under the definition of “fund”. However, if the remittance transaction of a Crypto Asset includes the exchange of fiat currencies in substance, such transaction will likely be deemed a money remittance transaction.

Anti-money laundering requirements

Under the APTCP, Exchange Providers are obligated to: (i) verify identification data of the customer and a person who has substantial control over the customer’s business for the purpose of conducting the transaction and occupation of business; (ii) prepare verification records and transaction records; (iii) maintain the records for seven years; and (iv) report suspicious transactions to the relevant authority, and so forth.

Promotion and testing

On June 15, 2018, the “Basic policy of Regulatory Sandbox scheme in Japan” was announced by the Cabinet Office of Japan. The Regulatory Sandbox is a scheme to implement new, outstanding technology such as AI, IoT, big data and blockchain, and welcomes new ideas for the “testing project” involving any industrial sector, inside and outside Japan.

Ownership and licensing requirements

There is no restriction on an entity simply owning cryptocurrencies for its own investment purposes, or investing in cryptocurrencies for its own exchange purposes. As a general rule, the Crypto Asset regulation under the PSA will not be applicable unless an entity conducts Exchange Services as a business. Please note, however, that the sale of certain types of tokens may be subject to regulation under the PSA or the FIEA, as applicable, as discussed in “Sales regulation” above.

Mining

The mining of cryptocurrencies is not regulated. Mining in itself does not fall under the definition of an Exchange Service. It should be noted, however, that if the mining scheme is formulated as involving CISIs and includes the sale of equity interests in an investment fund, it will be subject to the relevant FIEA regulations.

Border restrictions and declaration

Border restrictions

Under the Foreign Exchange and Foreign Trade Act of Japan, if a resident or non-resident has received a payment exceeding JPY30 million made from Japan to a foreign country or made from a foreign country to Japan, the resident or non-resident must report it to the Minister of Finance. If a resident has made a payment exceeding JPY30 million to a non-resident either in Japan or in a foreign country, the same reporting requirement applies.

On May 18, 2018, the Ministry of Japan announced that the receipt of payments in Crypto Assets or the making of payments in Crypto Assets, the market price of which exceeds JPY30 million as of the payment date, must be reported to the Minister of Finance.

Declaration

There is no obligation to declare cryptocurrency holdings when passing through Japanese Customs.

Reporting requirements

As explained above, a certain payment or receipt of payment exceeding JPY30 million, either by fiat currencies or Crypto Assets, is subject to a reporting obligation to the Minister of Finance under the Foreign Exchange and Foreign Trade Act.

An Exchange Provider must report to the relevant authority if it detects a suspicious transaction.

Estate planning and testamentary succession

There has been no established law or court precedent with respect to the treatment of cryptocurrencies under Japanese succession law. Under the Civil Code of Japan, inheritance

(i.e., succession of assets to heir(s)) occurs upon the death of the decedent. Theoretically, cryptocurrencies will be succeeded to by heir(s). However, given the anonymous nature of cryptocurrencies, the identification and collection of cryptocurrencies as inherited property would be a material issue unless the relevant private key or password is known to the heir(s). On the other hand, even if the private key or password is unknown, to the extent that the inherited property can be identified, theoretically, inheritance tax may be imposed. An enclosed and notarised testament may be one of the solutions for these issues. However, from the perspective of Japanese law, the legal framework must be improved so that these new issues can be adequately dealt with.



Taro Awataguchi

Tel: +81 3 6775 1104 / Email: taro.awataguchi@amt-law.com

Taro Awataguchi, a fintech partner at Anderson Mōri & Tomotsune (“AMT”), has extensive experience in advising clients, including Virtual Currency Exchange Service Providers (i.e., registered providers) and applicants for the registration, on various matters related to fintech and cryptocurrencies. AMT is one of the largest legal firms (Big Four) in Japan, and Taro, as a member of AMT’s fintech team which has one of the leading fintech practices in Japan, provides innovative, up-to-date legal advice to clients in this fast-growing and cutting-edge industry.

In addition, Taro was appointed by the Tokyo District Court as the trustee in bankruptcy proceedings of a Bitcoin-related company, where various legal issues and disputes related to Bitcoin were involved. He is a frequent speaker and author in the fintech field. For example, he made a speech on “Cryptocurrencies” at the American Bar Association (“ABA”) Section of International Law 2016 Fall Meeting held in Tokyo, and he is a co-author of the Japan Chapter of *International Comparative Legal Guide – Fintech* 2017 and 2018.

Taro already has extensive experience in the fields of banking, financing, financial regulation and insolvency. He is one of the pioneers of asset-based lending (“ABL”) practice in Japan, and serves as the head of the managing committee of the ABL Association. He is recognised by *Best Lawyers* (banking and financing law). He is noted for successful creditor representations in various cross-border insolvency matters, including representation of Japan’s first-ever secured creditors’ committee in getting full recovery from the corporate reorganisation proceedings of Spansion Japan Limited.



Takeshi Nagase

Tel: +81 3 6775 1200 / Email: takeshi.nagase@amt-law.com

Takeshi Nagase handles finance and corporate transactions, and has considerable experience advising on all legal aspects of public and private mergers and acquisitions, joint ventures, fintech, and other corporate and financial advisory matters. His clients range from prominent financial institutions to Crypto Asset start-ups. Between 2013 and 2014, Takeshi served on secondment in the disclosure department of the Financial Services Agency of Japan, where he was an instrumental part of the team that revised the laws and guidelines governing disclosure by listed companies, and prepared the Japanese Stewardship Code. Additionally, he handled a broad range of finance and corporate transactions on a secondment stint with the legal department of a major Japanese securities firm from 2015 to 2017. As a result of the unique perspective he has gained from these professional experiences, Takeshi is often sought for his advice on finance-related matters, particularly by clients seeking to evaluate transactions from the regulator’s point of view. Recently, Takeshi has extended his focus to Crypto Asset laws, including regulatory requirements applicable to registration of Crypto Asset Exchange Service Providers, initial coin offerings, and the like.

Anderson Mōri & Tomotsune

Otemachi Park Building, 1-1-1 Otemachi, Chiyoda-ku, Tokyo 100-8136, Japan

Tel: +81 3 6775 1000 / URL: www.amt-law.com

Jersey

Christopher Griffin, Emma German & Holly Brown
Carey Olsen Jersey LLP

Government attitude and definition

Jersey continues to embrace fintech including blockchain and distributed ledger technology (“**DLT**”) as a pioneer in fintech regulation. Jersey enjoys a sophisticated legal, regulatory and technological infrastructure, supporting development and innovation in fintech, including:

- payment services and online payment solutions;
- electronic identification (“**E-ID**”);
- virtual currency exchanges (“**VCEs**”) (cryptocurrency exchanges);
- security token exchanges;
- security token and non-security token issuances and initial coin offerings/security token offerings (“**ICOs**”/“**STOs**”);¹
- custody services and arrangements for holding digital assets; and
- fintech funds and other vehicles.²

Jersey recognised cryptocurrencies as a separate asset class long before the “ICO Craze” of 2017, when the Island’s regulator, the Jersey Financial Services Commission (the “**JFSC**”) licensed the world’s first Bitcoin-focused, regulated fund (GABI Plc). From that point onwards, the Island has seen a surge of interest in exchange vehicles, token issuers and fintech funds choosing Jersey, including the world’s largest investment fund (the SoftBank “Vision Fund” which raised \$97bn over two years). Both GABI and SoftBank were advised by Carey Olsen Jersey LLP (“Carey Olsen”).

The JFSC is a member of the Global Fintech Innovation Network and participates in the cross-border testing pilot.

Jersey has an exceptional pool of blockchain expertise, developed from the JFSC’s forward-thinking attitude combined with Jersey’s flexible range of corporate vehicles and favourable tax regime.

Examples of structures that have recently used Jersey (advised in each case by Carey Olsen) include:

- CoinShares Fund I, a venture capital fund investing in Ether (a cryptocurrency used as a payment on the Ethereum blockchain platform) and ICOs; and
- Binance, one of the world’s largest cryptocurrency exchanges, which has established a Jersey exchange platform.

In terms of trends in the past year pre-COVID-19, we are seeing an increased use of and enquiries about online payment solutions and E-ID and a continued interest in the establishment of cryptocurrency and security token exchanges. More recently, as a result

of COVID-19, we are seeing a sharp increase in the uptake of technology and new entrants to the market. Whilst not fintech as such, this includes a wide-spread use and adoption of electronic signatures (including witnessing) and a general shift towards digitisation and automation of manual procedures consistent with a wide-spread move to remote working. We are therefore expecting this trend to continue in the coming months and welcome the opportunities that this may present in terms of increased usage of blockchain and smart contracts and automation and AI in Jersey.

In terms of innovation generally, Jersey is striving to promote fintech development by supporting local fintech talent and innovation. Digital Jersey, a government-backed economic development agency and industry association dedicated to the growth of the digital sector, aims to do this. Further, the JFSC is a member of the Global Fintech Innovation Network and participates in the cross-border testing pilot. COVID-19 has also brought about pragmatic developments in Jersey's legal practice and has given rise to recent guidance from The Law Society of Jersey in relation to the signing of certain powers of attorney by electronic signature, which demonstrates Jersey's willingness to adopt technological developments.

Blockchain and cryptocurrency/digital asset regulation

To date, Jersey has not sought to introduce any fintech-specific legislation. The JFSC has sought to cater for fintech businesses within the existing regulatory framework until such time as there is a global consensus on how to regulate aspects of the fintech ecosystem; for example, if the fintech service involves the provision of a financial service, it will fall to be regulated within Jersey's financial services regime under the Financial Services (Jersey) Law 1998 ("**FSJL**") unless an applicable exemption is available. The FSJL defines "financial services business" as investment business, trust company business, general insurance mediation, money services business, fund services business or alternative investment fund services business.

The main types of fintech activities that are currently active in Jersey and require some level of regulatory oversight are:

- **Payment services** – depending on the payment services being offered, these may be required to be regulated under the FSJL to undertake "money services business", trust company business (as outlined above to the extent the services include an e-wallet relating to digital assets) or under the Banking Business (Jersey) Law 1991 for "deposit-taking" business. There are a number of exemptions that may apply and early advice should be sought.
- **VCEs** – these exchanges must maintain a registration under the Proceeds of Crime (Jersey) Law 1999 ("**POCJL**") as a "supervised business". The POCJL requires VCEs to comply with Jersey's laws, regulations, policies and procedures aimed at preventing and detecting money laundering and terrorist financing.
- **Security token exchanges** – these exchanges are required to be regulated under the FSJL to undertake "investment business" (an "**IB Licence**"). A standard application for an IB Licence will take approximately eight weeks. An application for a digital assets-related matter may take a little longer. A full regulatory application to the JFSC will be required and will include the following documents:
 - (a) a regulatory application form;
 - (b) a business plan; and
 - (c) a business risk assessment.

In terms of regulatory capital requirements, the main requirement to be aware of is that an exchange platform will be required to maintain at all times:

- (a) a net liquid assets position of 130% of its projected quarterly expenditure;
- (b) a minimum of £25,000 paid-up share capital; and
- (c) a minimum net assets position of £25,000 at all times.

In addition, a Jersey security token exchange must be audited and the composition of the board must comply with the Jersey regulatory and economic substance requirements, being:

- (a) there must be a minimum of two Jersey resident directors;
- (b) the board must meet with adequate frequency having regard to the amount of decision making being undertaken;
- (c) at meetings there must be a quorum of directors physically present in Jersey; and
- (d) the directors of the company must have the necessary knowledge and expertise to discharge their duties (this is assessed on a whole-board basis).

Once an IB Licence has been obtained, the holder will need to observe the provisions of the JFSC's Code of Practice for Investment Business.

- There are locally regulated administrators in Jersey who can assist by providing “incubation” services to entities and groups that are new to Jersey.
- There is no requirement to have electronic clearing and settlement or for clearing of security tokens to be carried out by a clearing house or central depository.
- The increase in uptake of exchange-related investment business in Jersey has resulted in the JFSC consulting on proposed amendments to the class of investment business to include a specific new category of exchange business. We await the outcome of the Consultation.
- **Custody services and arrangements for holding digital assets** – there are two models: (i) custody services provided by the exchange itself (or a related entity) to investors and exchange users; and (ii) custody services outsourced to a third-party custody provider to be provided to investors and exchange users.

In both models, where digital assets will be stored offline or where the investor or exchange user is not provided with the keys to access the digital asset, the investor/exchange user will no longer have control over the digital assets they have invested in. In this way, it is likely that the relevant custodian entity will be providing trustee services and will need to be regulated for “trust company business” under the FSJL. However, where the storage of digital assets is incidental or ancillary to the main purpose of the entity and where there was no separate remuneration, an exemption may apply. Early advice should be sought on this point, and this is something Carey Olsen has experience of advising on.

- **Business relating to digital assets and cryptocurrency** – “sensitive activity” – the JFSC will treat transactions with digital assets and cryptocurrencies as a “sensitive activity” under the JFSC's Sound Business Practice Policy. The practical consequence of this is that certain AML/CFT obligations are imposed on the issuer, such as to carry out checks on: (i) the purchasers of the tokens who purchase coins directly from the issuer; and (ii) the holders of tokens issued by the issuer in the event they are sold back to the issuer. In such circumstances, the issuer will be required to obtain information to: (a) establish and obtain evidence to verify identity; and (b) establish and, depending on the level of risk, obtain evidence to verify the source of funds and source of wealth.

Taxation

Jersey provides a stable, tax-neutral environment. Many Jersey companies (apart from locally regulated financial services companies and utilities) can be zero-rated for income tax

and are not subject to capital gains tax within the jurisdiction. Jersey has no capital transfer or similar taxes and does not levy any withholding tax on dividends. There is also no stamp duty on Jersey share transfers. Companies can also be incorporated in Jersey but can be resident for tax purposes in another jurisdiction if certain criteria are met.

There are currently no specific laws regulating the taxation of cryptocurrencies or digital assets, although Jersey's Comptroller of Taxes has issued guidance on cryptocurrency tax treatment regarding both Jersey income tax and Jersey goods and services tax. The guidance provides that such assets will be taxed in accordance with general Jersey taxation principles and provisions.

Promotion and testing

Jersey promotes and tests fintech firms' products and services in a number of ways.

In terms of testing products and services, the JFSC has proven itself to be a proactive and forward-thinking regulator in becoming a member of the Global Fintech Innovation Network (a group of international regulators and observers committed to supporting innovative products and services) and participating in the cross-border testing pilot that launched in January 2019, offering firms the opportunity to test their products and services in multiple jurisdictions.³

Jersey also operates a sandbox run through Digital Jersey, supporting local fintech firms and fintech firms seeking to relocate to Jersey.⁴

In terms of promoting fintech and thought-leading in Jersey, the Digital Assets Working Group (the "DAWG") works hard to raise awareness and interest in Jersey. Combining representatives of the States of Jersey, representatives of the JFSC and other interest groups on the Island, the DAWG is a group of individuals knowledgeable in the fintech space promoting digital assets and blockchain technologies in Jersey. Carey Olsen is a founder member of the DAWG and is an active participant and contributor.

Mining

Mining cryptocurrencies is not covered by any specific piece of legislation or regulation in Jersey. However, depending on the manner in which mining activities are conducted, it may fall within the existing regulatory framework for funds (mentioned above).

Border and reporting restrictions

At present, there are no border restrictions in place on declaring cryptocurrency holdings. Equally, there are currently no specific reporting requirements triggered for cryptocurrency payments.

The future of blockchain and DLT in Jersey

As a nascent technology, international industry practices around blockchain and DLT are still evolving and their applications and use cases (including outside the finance industry) being asserted. To maintain its place as a respected, well-regulated international finance centre, Jersey is cognisant, and encouraging, of the advantages blockchain and DLT bring to Jersey's finance industry.⁵

As a long-established, well-regulated international finance centre, Jersey boasts a host of industry experience and local expertise in Jersey,⁶ making it an ideal jurisdiction to launch new blockchain and DLT initiatives.

Leveraging this existing expertise and the low-tax environment, we expect to see Jersey and Jersey vehicles continue to be used in both established areas of finance as they embrace blockchain solutions (such as proptech, online settlement solutions, E-ID and regtech, etc.) and new areas of finance and other sectors as blockchain and DLT use cases are established. The JFSC's considered and measured approach to fintech regulation to date should equip Jersey to be a leading blockchain and DLT jurisdiction of the future by ensuring regulation in Jersey remains appropriate and commensurate to the product or service in question. We would be happy to discuss any blockchain or DLT initiatives backed by persons of substance. Please do contact us using the details below.

* * *

Endnotes

1. In the fintech space, the ICO terminology has now largely been superseded by reference to security and non-security tokens, a reflection of the evolving regulatory backdrop. We retain reference to ICOs in this chapter because we, Carey Olsen, have advised in relation to a number of ICOs and that was the terminology used at that time. The settled approach now is to determine whether a coin or token or other digital asset issued constitutes a security or not and therefore whether it is a "security token" or not. We have addressed STOs and non-security token issuances separately.
2. There is JFSC guidance available at https://www.jerseyfsc.org/media/2003/2018-07-12_jfsc-issues-ico-guidance-note.pdf. It has been confirmed that this JFSC Guidance has a wider application and can be used to inform how digital assets and cryptocurrencies more generally will be treated.
3. The window for applications to participate in the January 2019 pilot has now closed.
4. See: <https://www.digital.je>.
5. Such as: (i) real time settlement; and (ii) greater transparency as to origination or provenance of the asset in question. For example, as Jersey currently has no restrictions or requirements around financial settlement, Jersey is an ideal jurisdiction from which to launch securities and cryptocurrency exchanges.
6. Including in banking, international payments, compliance, funds, capital markets, real estate and company administration.

**Christopher Griffin****Tel: +44 1534 822 256 / Email: christopher.griffin@careyolsen.com**

Christopher spearheads Carey Olsen's crypto practice and digital assets team, advising on the launch in 2017 of CoinShares Fund I (a venture cap fund investing in crypto assets) and ARC Reserve Currency, Jersey's first initial coin offering or "ICO". Christopher was instrumental in the launch of the Jersey platform for Binance, the world's largest cryptocurrency exchange. Christopher also advises on all aspects of fund and corporate transactions, including the legal and regulatory aspects of fund launches, and joint ventures. He also has considerable experience in dealing with the Jersey Financial Services Commission in navigating investment vehicles through the Jersey regulatory approval process.

Christopher has broad experience of both general international corporate and funds work with particular expertise in private equity and hedge funds, having spent 10 years as a corporate and funds lawyer in the City.

**Emma German****Tel: +44 1534 822 474 / Email: emma.german@careyolsen.com**

Emma is a senior associate in the Carey Olsen Jersey digital assets team and has advised in relation to a number of blockchain and digital asset-related matters, including in relation to: payments, the establishment of virtual currency exchanges and security token exchanges; the use of Jersey vehicles for token issuances; and digital company administration in Jersey. Emma has a background in international corporate and finance transactions and her expertise includes the raising of finance through the issuance and listing of Eurobonds and other securities on The International Stock Exchange.

Emma is an advocate of the Royal Court of Jersey. She is a barrister of England and Wales (non-practising) and an English solicitor. She was educated at King's College London. Emma joined Carey Olsen in 2005. In 2016, she was seconded to The Royal Bank of Scotland International Limited.

**Holly Brown****Tel: +44 1534 822 231 / Email: holly.brown@careyolsen.com**

Holly is an associate in Carey Olsen's Jersey corporate department. She is a member of the digital assets team and has assisted with various matters related to cryptocurrencies/digital assets and blockchain, including the launch of Binance's Jersey exchange platform and in relation to payments. Holly also advises on the raising of finance by issuers and the listing of Eurobonds and other securities on The International Stock Exchange, having completed a secondment to The International Stock Exchange.

Holly is an advocate of the Royal Court of Jersey. She was educated at King's College London. Holly joined Carey Olsen in 2013.

Carey Olsen Jersey LLP

47 Esplanade, St Helier, Jersey JE1 0BD, Channel Islands
Tel: +44 1534 888 900 / Fax: +44 1534 887 744 / URL: www.careyolsen.com

Luxembourg

José Pascual, Holger Holle & Clément Petit
Eversheds Sutherland LLP

Government attitude and definition

The regulatory authority that oversees Luxembourg's financial sector, the *Commission de Surveillance de Secteur Financier* (the “**CSSF**”), acknowledges the financial benefits of blockchain technology, and Luxembourg's Minister of Finance, Mr. Pierre Gramegna, has spoken of the “added value and efficient services” that cryptocurrencies bring. Luxembourg is known for its proactive approach to blockchain technology, and in recent years has developed its regulatory framework in relation to crypto assets.

Cryptocurrency regulation

Luxembourg has sought to be a leader in the regulation of cryptocurrency markets by amending and updating its securities laws, in particular the Luxembourg law of 1 August 2001 on the circulation of securities and other fungible instruments, as amended (the “**2001 Law**”).

The 2001 Law was amended by the Luxembourg law of 6 April 2013 on “dematerialised securities” (the “**2013 Law**”) to allow Luxembourg companies and investment funds to issue securities in dematerialised form and convert existing registered or bearer securities (in individual or global form) into dematerialised securities.

Last year, the 2001 Law was further amended by the Luxembourg law of 1 March 2019 providing increased legal certainty by expressly permitting securities to be maintained by the account keeper through secured electronic registration mechanisms, including distributed ledger technology (“**DLT**”) such as blockchain (the “**2019 Law**”). The purpose of this 2019 Law is to enable financial market participants to benefit from opportunities offered by new technologies in the field of the circulation of securities.

The 2019 Law inserted a new Article 18*bis* into the 2001 Law (English translation):

“(1) The account keeper may hold securities accounts and register securities in securities accounts within or through secured electronic registration devices, including distributed electronic registers or databases. Successive transfers registered in such a secured electronic registration device are considered transfers between securities accounts. The holding of securities accounts within, or the registration of securities in securities accounts through, such a secured electronic registration device do not affect the fungibility of the securities concerned.

(2) Neither the application of this law, nor the location of the securities which continue to be held with the relevant account keeper, nor the validity or enforceability of the security interests or collateral arrangements created under the amended Law of 5 August 2005 on financial collateral arrangements shall be affected by the holding of

securities accounts within, or by the registration of securities in the securities accounts through, such a secured electronic registration device.”

As a result, account holders may now hold securities accounts and make registrations of securities through the use of secured electronic recording devices, including registers or DLT of the blockchain type. In particular, it enables the use of tokens in the form of digital assets stored in a blockchain. The commentary to the 2019 Law (“**Bill 7363**”) states that a “token” stored in a blockchain should be considered a new type of “electronic asset” representing the security, as in the case of a paper security or a traditional dematerialised security, and to which the same rights would legally apply as to traditional dematerialised securities. In that sense, successive registrations of securities in a blockchain have the same effect as that resulting from a registration of securities between securities accounts.

A key principle arising out of Bill 7363 is technological neutrality. Under this principle, the 2019 Law recognises the possibility of using different types of “*secured electronic registration devices*”, not just distributed electronic registers or databases (i.e. blockchain). Thus, even though there may be practical discussions on whether electronic registration devices other than distributed electronic registers or databases are secure, the 2019 Law allows a flexibility in relation to new technologies which would have been limited if the 2019 Law adopted a precise definition.

The possibility of issuing dematerialised securities through distributed electronic registers or databases is not expressly recognised under the 2019 Law; however, this is addressed by the draft bill of Law 7637 on the issuance of dematerialised securities using DLT (“**Bill 7637**”), which was published by the Luxembourg government on 27 July 2020. Bill 7636 will modify the law of 5 April 1993 on the financial sector, as amended (the “**Financial Sector Law**”) as well as the 2019 Law. It will introduce the following changes:

- It incorporates a definition of “securities issuance accounts” (*compte d’émission*) in the 2013 Law, confirming that such securities issuance account may be held within or through secured electronic registration devices, including distributed electronic ledgers or databases. Thus, Bill 7637 would allow the reliance on DLT for both securities accounts and also issuance accounts in the context of an issuance of dematerialised securities. A securities issuance account is an account held with a settlement provider or central account keeper which can be held and allows for the recording of dematerialised securities by secured electronic recordings (including DLT).
- Provided they meet certain specific organisational and technological requirements, Bill 7637 opens up access to the activity of central account holders (*teneur de comptes central*) to EU credit institutions and investment firms within the meaning of the Financial Sector Law.

Bill 7637 greatly reinforces Luxembourg’s legal framework for the issuance and circulation of securities within the realm of DLT and encourages the use of new technologies in financial services.

Sales regulation

On 14 March 2018, the CSSF issued a warning on virtual currencies, indicating that, even though there was no legal framework in Luxembourg that specifically applied to virtual currencies, it should be borne in mind that any provision of financial services requires authorisation by the Minister of Finance.

In another warning issued on the same date relating to initial coin offerings (“**ICOs**”) and tokens, the CSSF acknowledged that raising funds from the public in the form of ICOs is

not subject to specific regulation, and does not benefit from any guarantee or other form of regulatory protection. The CSSF considered that despite the lack of specific regulations applying to ICOs, activities related to the creation of tokens and the collection and raising of funds may, depending on their characteristics, be subject to certain legal provisions and thus to a number of supervisory requirements.

The CSSF specified in the second warning that it would “*assess such fundraising activities by extending its analysis to the objectives pursued in order to assess whether it could be a scheme to circumvent or avoid financial sector regulations, notably the provisions of the Law of 10 July 2005 on prospectuses for securities and the Law of 5 April 1993 on the financial sector. The CSSF considers that for any fundraising, the initiators of such ICOs are required to establish anti-money laundering and terrorist financing procedures*”.

For more details on the applicable framework in relation to anti-money laundering and counter-terrorist financing, please refer to the “*Money transmission laws and anti-money laundering requirements*” section below.

As the CSSF does not provide for a classification of virtual currencies, the CSSF warning was in line with the European Securities and Markets Authority (the “**ESMA**”) position on ICOs (ESMA statement of 13 November 2017 ESMA 50-157-828, the “**ESMA Statement**”), which considered that firms involved in ICOs must give careful consideration to whether their activities constitute regulated activities.

According to the ESMA Statement, the coins or tokens used as crypto-assets may qualify as financial instruments. It is likely that the firms involved in ICOs conduct regulated investment activities, such as placing, dealing in or advising on financial instruments or managing or marketing collective investment schemes. Moreover, they may be involved in offering transferable securities to the public.

This position was later confirmed in ESMA advice on ICOs and crypto-assets dated 9 January 2019 by stating that although there is no legal definition of a crypto-asset, it could potentially be subject to a range of legal provisions when they qualify as transferable securities and/or other types of financial instruments.

Taking as a starting point the CSSF’s warning on ICOs, an ICO may fall within the scope of the Financial Sector Law, the Luxembourg law on markets in financial instruments, the Luxembourg law relating to undertakings for collective investment (the “**UCI Law**”) and the Luxembourg law on prospectuses for securities.

A token could also be structured in such a way as to qualify as a unit in an investment fund, as defined by the UCI Law relating to undertakings for collective investment. A token could also be based on or represent a unit in an alternative investment fund and thus trigger the requirement to structure such fund in consideration of the Luxembourg law on alternative investment fund managers.

Where a token qualifies as a financial instrument within the meaning of the Financial Sector Law, the provision of investment and ancillary services in and from Luxembourg may trigger the requirements to obtain prior written authorisation from the CSSF, including, *inter alia*, to act as portfolio manager, investment adviser, underwriter of financial instruments, or broker in financial instruments.

If a token qualifies as a security within the meaning of (44) of Article 4(1) of Directive 2014/65/EU and is offered to the public or admitted to trading on a regulated market, the issuance of such virtual currencies is not permitted prior to the publication of a prospectus which has been approved by the CSSF under the Luxembourg law on prospectuses for securities.

Finally, where a token matches the definition of electronic money within the meaning of the law of 10 November 2009 on payment services, as amended (the “**Payment Services Law**”), the issuer must apply for licence or registration with the CSSF to provide services or issue electronic money.

Taxation

In recent years, the Luxembourg tax authorities aimed at clarifying the direct taxation and VAT treatment of cryptocurrencies.

Luxembourg income taxation

In a circular published on 26 July 2018 regarding virtual currencies, the Luxembourg tax authorities highlighted that a cryptocurrency is not a currency, it is not legal tender and its value is not monitored by any central bank. Therefore, for direct tax purposes, it constitutes an intangible asset, meaning that companies will not be allowed to draw up their financial statements or to file their tax returns in cryptocurrencies.

This circular goes on to state that when a cryptocurrency is used as a payment method, the nature of the income will not be affected. This means that, for example, where rent is paid in virtual currency, it does not affect the nature of rental income.

When income is derived from disposing of the cryptocurrency itself, taxation of such income does not depend on whether it has been accrued in the real or virtual world, but whether the derived income is commercial income or “other income”.

The income derived from cryptocurrencies will constitute “commercial income” providing that it meets the conditions set out in Article 14 of the Luxembourg law dated 4 December 1967 on income tax (the “**Income Tax Law**”): “*Any independent activity, with a profit-making intention, exercised on a permanent basis, which participates in the general economy, when said activity is neither a forestry activity nor an independent professional activity.*” In this respect, there are three categories of taxpayers:

Category 1: Luxembourg corporate taxpayers

Luxembourg corporate taxpayers carry on a commercial activity. Therefore, the gains of such taxpayers derived from the disposal of cryptocurrencies will constitute commercial income. Such commercial income will be fully taxable at a combined corporate income tax and municipal business tax rate of 24.94% (combined tax rate for a corporate taxpayer based in Luxembourg City).

Category 2: Luxembourg individual taxpayers

The gain realised on the disposal of cryptocurrencies by Luxembourg individual taxpayers carrying on a commercial activity will constitute commercial income. Such income will be taxable at the progressive tax rates applicable for personal income tax, varying from 0% to 42%.

If the Luxembourg individual taxpayer does not carry on a commercial activity, the gain realised on the disposal of cryptocurrencies should be considered “other income”. If this “other income” is realised within six months after the acquisition of the cryptocurrency, such income will be considered a speculative gain and will be fully taxable at the applicable progressive tax rates for personal income, varying from 0% to 42%. However, if the gain is realised six months after the acquisition of the cryptocurrency, such gain will be exempt from Luxembourg personal income tax.

Category 3: Luxembourg partnerships

Luxembourg partnerships are tax transparent from a Luxembourg tax perspective unless they are considered to carry on a commercial activity. Under this context, a Luxembourg partnership not carrying on a (deemed) commercial activity should not be subject to Luxembourg taxation for the gains realised on disposal of cryptocurrencies. However, if a Luxembourg partnership is considered to realise commercial income, such commercial income will be subject to municipal business tax at a rate of 6.75% (for a Luxembourg partnership based in Luxembourg City).

Value-added tax

In addition, in June 2018, the Luxembourg VAT authorities published Circular No. 787 regarding exemption for virtual currency transactions, stating that the VAT exemption applicable to transactions concerning currency used as legal tender would extend to virtual currencies, to the extent that they are regarded as a method of payment and are accepted for this purpose by some operators.

Money transmission laws and anti-money laundering requirements

The Luxembourg legislator recently implemented two new laws to strengthen the anti-money laundering and counter-terrorist financing framework. These amend the Luxembourg law of 12 November 2004 on anti-money laundering and counter-terrorist financing (the “**AML/CFT Law**”) and introduce new registration and governance requirements for virtual asset service providers (“**VASPs**”), which must be registered with a register (the “**Register**”) established by the CSSF and published on its website.

The AML/CFT Law provides a broad definition of VASPs that covers all entities providing one or more of the following services on behalf of their clients or for their own account:

- exchange between virtual assets and fiat currencies, including the exchange between virtual currencies and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, including custodian wallet services; and
- participation in and provision of financial services related to an issuer’s offer and/or sale of virtual assets.

The AML/CFT Law defines “virtual asset” as a digital representation of value, including a virtual currency, that can be digitally traded or transferred, and can be used for payment or investment purposes. However, the definition of virtual assets does not include assets that fall within the meaning of electronic money under the law of 10 November 2009 on payment services (the “**2009 Law**”) or assets that qualify as financial instruments under the Financial Sector Law.

A “virtual currency” is a digital representation of a value that is neither issued nor guaranteed by a central bank or other public authority, is not necessarily linked to a legally established currency, and does not have the legal status of currency or money, but which is accepted as a means of exchange by persons and can be transferred, kept safe and exchanged electronically. Finally, the “custodian wallet service” is a service consisting of safekeeping private cryptographic keys on behalf of clients for the purpose of holding, safekeeping and transferring virtual currencies.

For the purpose of registration with the Register, VASPs must send a request to the CSSF, together with the following information:

- the name of the requesting entity;
- the address of the central administration of the requesting entity;
- a description of the services provided and the activities performed, and the list of the specific virtual asset services provided; and
- a description of the money laundering and terrorist financing risks that the requesting entity will be exposed to and of the internal control mechanisms that the requesting entity implements to mitigate those risks, and to comply with the professional obligations included in the AML/CFT Law and in Regulation (EU) No. 2015/847 on information accompanying transfers of funds.

To successfully obtain registration, a VASP must submit evidence of the professional repute of the individuals exercising management functions in the VASP and its ultimate beneficial owners (“UBOs”) to the CSSF. There must be at least two individuals exercising management functions who must be empowered to effectively determine the direction taken by the business and possess adequate professional experience. Any change to the UBOs or individuals exercising management functions must be pre-approved by the CSSF.

The CSSF has the right to remove the entity from the Register in case of non-compliance with certain obligations and has the power to impose administrative sanctions and other administrative measures in the AML/CFT Law.

Promotion and testing

In line with its technology-neutral position, the CSSF chose not to regulate the underlying technology or the cryptocurrencies themselves, but rather the service providers who offer financial services involving cryptocurrencies.

The first European exchange platform, Bitstamp, which enabled customers to exchange bitcoin against EUR and USD and *vice versa*, was authorised by the Luxembourg Minister of Finance in April 2016 to operate EU-wide bases under a payment institution licence. One of the largest exchanges in the world – bitFlyer – received its Luxembourg licence in December 2017, becoming the first bitcoin exchange to be licensed on three continents.

Ownership and licensing requirements

In the current framework of the Luxembourg fund industry, although very flexible, no regulated investment fund is currently used for investing in crypto-assets or virtual currencies.

Nevertheless, there are some unregulated investment vehicles that have been set up to invest directly or indirectly in crypto-assets or virtual currencies.

Mining

There are no restrictions in Luxembourg on the mining of cryptocurrency, provided that the production of such virtual currencies/crypto-assets does not fall within the scope of any specific statutory licensing obligation. Please refer to the “*Sales regulation*” section above.

Border restrictions and declaration

In line with the CSSF warning regarding virtual currencies, which states that “*given the cross-border character of VC transactions, establishing a national regulation would only*

have limited effects”, there are no specific border restrictions or any obligations to declare cryptocurrency holdings under Luxembourg law.

Reporting requirements

Under Luxembourg law, there is no reporting requirement for crypto-asset payments regardless of transaction value.

Estate planning and testamentary succession

Under Luxembourg law, there is no special treatment for crypto-assets for the purposes of estate planning and testamentary succession, and crypto-assets should be treated like any other assets in such situations.

* * *

Acknowledgment

The authors wish to acknowledge the valuable contribution of David Darvishi to this chapter. David works in the financial institutions department of Eversheds Sutherland (Luxembourg) LLP and specialises in investment funds. His main areas of practice include formation and ongoing assistance of investment funds, especially AIFs including private equity and real estate funds, financial services matters, regulatory issues (AIFMD, UCITS V, MiFID II, etc.), company law, the setting up of portfolio management companies and cross-border marketing issues. David holds an LL.M. in international business law from Queen Mary University of London (England), a Master’s degree in French and German business law from Paris Nanterre University (France), and an LL.B. from the University of Potsdam (Germany).

**José Pascual****Tel: +352 278 64695 / Email: josepascual@eversheds-sutherland.com**

José Pascual is the managing partner in Eversheds Sutherland (Luxembourg) LLP and specialises in investment funds formation work, advising domestic and foreign clients on matters relating to the structuring, setting up and organisation of AIFs (whether regulated or non-regulated). This includes contracts, company law, regulatory matters and operating arrangements, with a specific focus on private equity funds, real estate funds, infrastructure funds, hedge funds, debt funds and any other type of alternative assets funds, as well as the related acquisition structures. He is also deeply involved in the corporate and transactional aspects relating to such alternative funds and the structures set up for acquisition purposes.

**Holger Holle****Tel: +352 278 64696 / Email: holgerholle@eversheds-sutherland.com**

Holger Holle is a partner in Eversheds Sutherland (Luxembourg) LLP's corporate group. He divides his time between the firm's Luxembourg office, where he leads the corporate practice, and the Munich office. Holger focuses on business and corporate law and particularly specialises in national and cross-border mergers and acquisitions and private equity transactions.

Holger's experience includes advising: NYSE-listed WestRock Company and the acquisition by WestRock of Multi Packaging Solutions International Limited; the Teacher Retirement System of Texas on the acquisition of KBC Bank Deutschland and the acquisition of Oldenburgische Landesbank by Bremer Kreditbank; a leading New York private equity house on structuring and financing in relation to several investments in Europe; and the private equity investors in the sale of Nycomed Group by the Luxembourg holding entity Nycomed SICAR and the subsequent exit from the SICAR.

**Clément Petit****Tel: +352 278 64683 / Email: clementpetit@eversheds-sutherland.com**

Clément Petit is an associate in the financial institutions department of Eversheds Sutherland (Luxembourg) LLP and specialises in regulated and non-regulated investment funds with a focus on undertakings for collective investment in transferable securities (UCITS), as well as alternative investment funds and AIF managers under the Alternative Investment Fund Managers Directive (AIFMD). In addition, he worked as secondee in an international Swiss bank on the acquisition of another Luxembourg-based bank and as an AIF manager on AML/CFT aspects. Clément was admitted to the Luxembourg Bar in October 2018 and holds a Master's degree in International Business Law from the Nancy Faculty of Law (France) and an LL.M. degree in International Commercial Law from Swansea University (Wales).

Eversheds Sutherland LLP

The Marivaux, 33, Rue Sainte Zithe, L-2763, Luxembourg
Tel: +352 278 64700 / URL: www.eversheds-sutherland.com

Mexico

Carlos David Valderrama Narváez, Alejandro Osornio Sánchez &
Diego Montes Serralde
Legal Paradox®

Government attitude and definition

On March 9th, 2018, the Mexican Government published in the Mexican *Official Federal Gazette* the law that regulates Financial Technology Institutions (ITFs), also known as the Fintech Law (which entered into force the following day). This new law regulates the operation of virtual assets (commonly known as cryptocurrencies) within the Mexican financial system, which defines them as “the representation of value electronically recorded and used among the public as a payment method for any kind of legal act and whose transfer can only be carried out through electronic means”. Notwithstanding the foregoing, the same law sets forth that in no case shall virtual assets be understood as currency of legal tender on national territory, foreign currency or any other asset denominated in legal tender or in foreign currency.

In this regard, the following comments are made to clarify the scope of the law:

1. The Fintech Law only provides the legal framework for financial entities (ITFs and banks) to perform operations with virtual assets (see below for more details).
2. The Mexican Central Bank (Banxico) is legally entitled to determine in secondary regulation the characteristics that the virtual assets must fulfil to be used by the financial entities mentioned above.

Having said that, with the enactment of the Fintech Law, Mexican financial authorities took a first step to recognising the use of virtual assets within the Mexican financial system. However, in March 2019, the Financial System Stability Council (composed of the Ministry of Finance, the Mexican Central Bank, the National Banking and Securities Commission, the National Insurance and Bonding Commission, the National Retirement Savings System Commission and the Bank Savings Protection Institute) decided to adopt a conservative stance regarding this, considering that there should be a healthy distance between virtual assets and the Mexican financial system.

Notwithstanding the foregoing, financial authorities have also expressed that it is important to allow the admission of new technologies. In this context, the Regulatory Sandbox will be an important tool to foster the emergence of those (for example, blockchain technology). Moreover, the operation with virtual assets by non-financial entities is allowed in accordance with the terms listed on the Federal Law for the Prevention and Identification of Operations with Resources of Illegal Proceeds (also known as the Anti-money Laundering Law) (see below for more details).

Finally, as of the date of preparation for this chapter, there are no virtual assets supported by either the Mexican Government or by Banxico.

Cryptocurrency regulation

As mentioned above, the Fintech Law provides the legal framework for financial entities to operate with virtual assets. However, this law also regulates several exciting tools that promote innovation within the Mexican financial system:

1. It creates the financial entities known as ITFs:
 - I. Crowdfunding Institutions: their purpose is to facilitate communication between applicants and investors so that the latter can provide resources to the former for specific projects. The law regulates both lending and equity activities.
 - II. Electronic Money Institutions: their purpose is the issuance, administration, redemption and transmission of electronic money for payments or transfers of funds.
2. Virtual assets: according to the Fintech Law, both ITFs and banks may perform operations using virtual assets, prior recognition, and authorisation from Banxico.
3. Innovative Models (also known as Regulatory Sandboxes): these authorisations allow both financial and non-financial entities to carry out regulated activities using innovative technological tools or means with different modalities from those currently existing in the Mexican market and with a lower regulatory burden (see below for more details).
4. Application Programming Interfaces (APIs): this tool allows financial entities to share information with other financial entities or third parties to improve the customer's experience. This will give rise to the model known as "open finance", as opposed to the traditional model of "open banking".

Notwithstanding the foregoing, the legal framework for virtual assets also includes the Federal Law for the Prevention and Identification of Operations with Resources of Illegal Proceeds. This law regulates the operations with virtual assets performed by non-financial entities, considering these as vulnerable activities (see below for more details).

Finally, on March 8th, 2019, Banxico published in the Mexican *Official Federal Gazette* the secondary regulation known as "Circular 4/2019" whose main purpose is to determine the characteristics that virtual assets must fulfil in order to be used between financial entities (ITFs and banks) and their customers. Nevertheless, as of September 2020, Banxico has not determined any virtual assets that can be used under these conditions within the Mexican financial system. However, these financial entities can use the technology on which virtual assets are based in accordance with the terms listed in "Circular 4/2019".

Sales regulation

In Mexico, there are no official categorisations other than the definition of virtual assets as a "representation of value electronically recorded and used among the public as a payment method for any kind of legal acts and whose transfer can only be carried out through electronic means" set forth in the Fintech Law.

The use of virtual assets is regulated by the Fintech Law and by anti-money laundering (AML) regulations, but there are other tokens, like stablecoins, that do not fulfil the requirements to be considered virtual assets pursuant to the Fintech Law. In this context, it is important to analyse whether the asset has the qualities of a security under the Mexican regulatory framework, in which case that framework will be applicable.

Taxation

As of the date of preparation of this chapter, there is no specific tax regulation issued for cryptocurrency; as a consequence, the corresponding tax impact must be analysed on case-by-case basis.

In general terms, all persons in Mexico – whether individuals or companies – are obliged to contribute to public expenses, in accordance with the respective laws. There are several federal contributions that must be taken into account when making an investment in our country, among which are income tax and value-added tax.

Income tax is a direct contribution levied on income received by residents in Mexico and residents abroad with or without a permanent establishment in the country. This tax is calculated by applying a rate of 30% to the taxable base determined in accordance with the parameters of the law. In the case of residents abroad without an establishment in Mexico, the tax is generally paid by means of a withholding.

The legislation governing this tax sets forth cases of accumulation of income, deductions from income, as well as schemes which, depending on the operation, have special characteristics.

Value-added tax, as an indirect tax, is levied on the consumption of goods and services under various headings, such as the sale of goods, the provision of services, the granting of temporary use or enjoyment of goods and the importation of merchandise. This tax is currently levied at a general rate of 16% on the values established for calculating the tax in each case. This tax is caused by the person who disposes of goods, provides services or grants the temporary use or enjoyment of goods, and must transfer it and collect it from the person who acquires the good or service, or the lease, as the case may be.

It is also relevant to note that one of the most important attributes for both taxes is the residence of the active subjects, as it links them to the jurisdiction of the State that exercises its taxing power. In Mexico, tax residents are considered to be legal entities that have established in the country the main administration of their business, and individuals, as a general rule, who establish their home in Mexico or are nationals of the country, although this must be analysed on a case-by-case basis to determine such tax residence.

Money transmission laws and anti-money laundering requirements

When talking about the “know-your-customer” (KYC) and AML legal framework applicable to transactions in digital assets, it is important to distinguish who is the entity making those transactions: (i) fintech and banking institutions; or (ii) other entities or natural persons.

For fintech and banking institutions, there are specific KYC/AML rules for each financial entity and, for other entities and natural persons, the general rules of the Federal Law for the Prevention and Identification of Operations with Resources of Illegal Proceeds apply.

The obligations for fintechs and banks are highly strict and have requirements such as the development of an AML Prevention Manual, the formation of internal structures in charge of the AML department, being the Compliance Officer and the Communication and Control Committee, and a risk-based approach analysis, among others.

The obligations for other entities and natural persons are more flexible, but they are subject to report transactions that exceed a predetermined threshold in one transaction or in the accumulated transactions of six months. For more information, please refer to the “Reporting requirements” section below.

Promotion and testing

The Regulatory Sandbox, included in our Fintech Law under the figure of Innovative Models, is promoting the creation of financial institutions with the use of state-of-the-art technology, highlighting blockchain as the most used.

The regulation in question implies a change in the regulatory paradigm in Mexico, as our financial law has its origin in civil and Roman law, a system of codified laws that attempts to cover in an exhaustive way each area of application for the law that can generate legal consequences. Opposed to the above, the Mexican Regulatory Sandbox is configured in such a way that it can even provide an *ad hoc* legal framework.

The Regulatory Sandbox, which is a business model that seeks to carry out an activity reserved for financial entities authorised by the Mexican financial regulator using innovative technological tools or means or with different modalities from those existing in the Mexican market, provides the applicant with a safe space to carry out tests with financial services in a real, temporary, controlled environment and above all with less regulatory burden. This is achieved by obtaining a temporary authorisation that will allow you to offer financial services.

It is important to note that we recently had the Sandbox Challenge, the first contest of entrepreneurship and financial innovation that encourages world-class entrepreneurs to test their business models in the Mexican financial system.

The Sandbox Challenge was organised by the UK Embassy and executed by Dai Mexico under the umbrella of the Financial Service programme, where Legal Paradox® acted as a sponsor, hand in hand with giants like Google, MassChallenge, ALLVP, among others.

Among the more than 400 people who downloaded the competition rules for the Sandbox Challenge, the use of blockchain technology was the favourite means of innovation, followed by artificial intelligence.

For more information, please refer to Valderrama, Carlos, 2020, “*Regulatory Sandbox: The cornerstone for the fintech disruptive innovation’s explosion in Mexico*”, at Rocio Haydee Robles Peiro, Fintech Law, context, content and implications, Mexico City, Mexico, Tirant lo blanch.

Ownership and licensing requirements

The restrictions for owning cryptocurrencies are only for financial institutions. The Fund Managers and Investment Advisors are considered financial institutions pursuant to the Stock Market Law and the Investment Funds Law, so they are not entitled to operate with virtual assets under the Fintech Law. The only financial institutions entitled to operate with virtual assets are banks and fintechs (ITFs).

The Investment Advisors are persons who, without being securities market intermediaries, habitually and professionally provide portfolio management services by taking investment decisions in the name and on behalf of others, as well as habitually and professionally providing investment advice in securities, analysis and issuance of investment recommendations on an individual basis. In this regard, if the cryptoasset is not considered a virtual asset under the Fintech Law, it could be considered a security with which the Investment Advisor or the Fund Manager could operate.

Notwithstanding the above, the Investment Funds Law established that the assets subject to investment have to be securities, titles and documents to which the regime of the Stock Market Law is applicable, registered in the National Registry or listed in the International Quotation System.

On the other hand, there are no restrictions or licence requirements for non-financial entities and natural persons to own cryptocurrencies; they only are obliged to comply with the

report requirements. For more information, please refer to the “Reporting requirements” section below.

Mining

There are no specific rules applicable to mining. However, in Mexico, a general principle applies: whatever is not prohibited by law is permitted for non-regulated people or businesses. Therefore, as there are no regulations or prohibitions applicable to mining, it is a permitted activity.

Notwithstanding the above, mining has an important energy aspect and, depending on the amount of energy required, a mining entity may be considered a qualified user and therefore subject to the corresponding energy legal framework.

Border restrictions and declaration

In Mexico, there are no specific rules applicable to border restrictions or obligations to declare cryptocurrency holdings.

However, it is important to mention that, from a fiscal perspective, our system is based on fiscal self-determination, as well as that certain reports are applicable from a regulatory perspective (see the “Reporting requirements” section below).

Reporting requirements

Reports issued by non-financial entities

The exchange of virtual assets made by non-financial entities in a habitual and professional way is regulated by the Federal Law for the Prevention and Identification of Operations with Resources of Illegal Proceeds. This law provides that non-financial entities must inform the Ministry of Finance when the amount of a trading transaction performed by a client is equal to or greater than 645 Update and Measurement Units (MXN 56,037.60 for 2020 – approximately USD 2,536.78).

Reports issued by ITFs (currently in force but inoperative, see “Cryptocurrency regulation” above for more details)

According to the AML/CFT (counter-terrorism financing) secondary regulation applicable for ITFs, these entities must share a report with the Ministry of Finance (through the National Banking and Securities Commission) within the first 10 business days of each quarter when a client has traded virtual assets for legal tender or foreign currency and *vice versa*, as long as the amount of the transactions made in a quarter have been equal to or greater than 7,500 Investment Units (these are units of measurement that vary according to inflation and are determined periodically by Banxico) (as of September 30th, 2020, this amount was MXN 49,121.84 – approximately USD 2,223.71).

Reports issued by banks (currently in force but inoperative, see “Cryptocurrency regulation” above for more details)

According to the AML/CFT secondary regulation applicable for banks, these entities must share a report with the Ministry of Finance (through the National Banking and Securities Commission) within the first 10 business days of each quarter when: (1) a client has bought a virtual asset using legal tender or foreign currency, no matter the amount of the transaction; and (2) a client has sold a virtual asset in exchange for legal tender or foreign currency, as long as the amount of the transaction made has been equal to or greater than USD 2,250.

Estate planning and testamentary succession

First of all, there are no specific rules applicable to estate planning and testamentary succession for cryptocurrencies; however, the general principles may apply.

In order to specify a legal treatment, we have to establish the legal nature of a virtual asset, being an intangible asset or good in which the owner has a property right.

In Mexico, inheritance is the succession of all property of the deceased and in all his rights and obligations that are not extinguished by death. In addition, inheritance is defended by the will of the testator or by provision of the law. The first is testamentary, and the second is legitimate.

Regarding natural persons, property rights for cryptocurrencies could be transferred by testamentary succession or by legitimate succession. However, there are no specific provisions regarding a custodial exchange to specify a beneficiary of the virtual assets in case of death, but as good practice, there are some custodial exchanges that grant that benefit to the heirs.

Now, with respect to non-custodial exchanges, there are no specific obligations. The cryptocurrency owner must transfer the private keys to the heir for a cold or hot wallet.

Finally, regarding banks and fintechs, the Fintech Law established that in the event of the customer's death, the fintech will deliver the amount corresponding to the electronic payment funds to which the customer himself has designated as beneficiaries, expressly and in writing, in the percentage stipulated for each of them, and the electronic payment funds could be also referred to virtual assets with the corresponding authorisation of the Mexican Central Bank.

**Carlos David Valderrama Narváez****Tel: +52 1 416 690 48 / Email: carlos@legalparadox.com**

Carlos is the founder and managing partner of Legal Paradox® with expertise in decentralised finance (DeFi), self-sovereign identity (SSI), regulatory sandboxes, stablecoins, wallets, crowdfunding, exchanges and broker-dealers, blockchain, KYC/AML rules, investment funds and smart contracts (even programming them in solidity and hyperledger). He provides advice to private and public entities such as the British Blockchain Association, as a member of its Advisory Board (2017–20) and a Regional Adviser, and the British Chamber of Commerce, as a member of its Financial Committee. He is part of the global alliance LACCHAIN, an initiative of the Interamerican Development Bank to promote the use of blockchain in Latin America and the Caribbean. Carlos lectures on blockchain at universities in Mexico and Latin America such as Universidad Panamericana and ITAM, as well as training judges at the Mexican Federal Judicial Institute, and officials of the Mexican Central Bank.

**Alejandro Osornio Sánchez****Tel: +52 1 416 690 48 / Email: alex@legalparadox.com**

Alejandro is a senior associate at Legal Paradox® with expertise in fintech including crowdfunding, electronic wallets and regulatory sandboxes. Prior to its incorporation to Legal Paradox®, Alejandro worked at the Mexican Ministry of Finance where he participated in the discussion and creation of the law that regulates Financial Technology Institutions (Fintech Law) as well as in the secondary regulation for regulatory sandboxes. Likewise, he participated within the fintech authorisation processes and has been a speaker at several national and international discussion forums on this subject.

**Diego Montes Serralde****Tel: +52 1 416 690 48 / Email: diego@legalparadox.com**

Diego is a junior associate at Legal Paradox® whose practice focuses on fintech authorisation processes before Mexican financial regulators, AML assessment, Data Protection assessment and blockchain projects. He has worked on a variety of fintech and financial projects, including Legal Paradox®'s own developments. He is currently working on a paper on blockchain and crypto regulation in LATAM, an initiative led by Legal Paradox®, and he contributed directly to the FinTech Map, a development by Legal Paradox®, which identifies more than 670 institutions operating in the Mexican fintech sector. He has also published several posts on the firm's blog, which have subsequently been taken up and published by Mexican and international media.

Legal Paradox®

Volcano 150, Floor 5, Lomas de Chapultepec, Mexico City, 11910, Mexico

Tel: +52 1 416 690 48 / URL: www.legalparadox.com

Montenegro

Jovan Barović, Luka Veljović & Petar Vučinić
Moravčević Vojnović i Partneri AOD
in cooperation with Schoenherr

Government attitude and definition

The Central Bank of Montenegro (“CBM”), the Capital Markets Commission (“CMC”) and the Ministry of Finance, as the most competent State authorities, have not yet issued any official guidelines or policy papers pertaining to cryptocurrencies. Other Governmental bodies have also been rather silent on the issue.

Montenegro is a candidate for membership in the European Union and a frontrunner in the accession process. Montenegro also applies the Euro as its legal tender even though the country is not a member of the Eurozone. Given the country’s strong desire to join the European Union, the competent State authorities tend to align their official positions with current European positions and legislation, which, in the area of cryptocurrencies, still remains reserved and to a certain extent doubtful, mostly due to the anonymity surrounding cryptocurrencies, which may lead to potential money laundering, terrorist financing and tax evasion.

Cryptocurrencies are not regarded as an official means of payment in Montenegro, although their possession and/or use is not prohibited.

The CBM, as the institution responsible for monetary policy and regulating the banking system, stated in a press release that virtual currencies are not a legal means of payment in Montenegro, and that any transactions facilitated through such currencies are performed at one’s own risk. The CBM also confirmed that it does not have information on how many individuals and companies are issuing and managing these currencies, or how many transactions are being made in the country. According to the CBM, cryptocurrencies did not have an impact on the banking system and they are not perceived as a threat to the banking system.

As to the issue of treatment of cryptocurrencies, there is no clear position.

The Vice Governor of the CBM has expressed his opinion that cryptocurrencies have more characteristics of electronic securities than characteristics of money. Namely, it seems that the understanding of the CBM is that cryptocurrencies lack important functions of money, since:

- they have limited function of means of payment;
- they are not units of account; and
- they do not store value.

However, the possibility that cryptocurrencies might obtain those characteristics at some point was not excluded. It should be noted, however, that this is not the official position of the CBM, but only the opinion expressed by its Vice Governor.

The CMC is yet to form a position on the issue of treatment of cryptocurrencies and whether they are financial instruments in the meaning of Montenegrin capital markets legislation.

Amendments to the Montenegrin Prevention of Money Laundering and Financing of Terrorism Act (*Zakon o sprječavanju pranja novca i finansiranja terorizma*) (“**AML Act**”) have introduced a definition of virtual currencies in the Montenegrin legal system in line with Directive (EU) 2018/843 of the European Parliament and of the Council dated 30 May 2018. In accordance with the AML Act, virtual currencies are defined as digital representations of value that are not issued by the CBM or a public authority, are not necessarily attached to a conventional currency, but are accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically. In accordance with current European practice, cryptocurrencies are considered to be one form of virtual currency. Additionally, the Rulebook on indicators for recognising suspicious clients and transactions (*Pravilnik o indikatorima za prepoznavanje sumnjivih klijenata i transakcija*) explicitly lists some cryptocurrencies as virtual currencies (Bitcoin, Litecoin). Interestingly, however, the legislator did not transpose one important part of the Directive into the AML Act which expressly defines that virtual currencies do not possess the legal status of currency or money.

Currently, there are no cryptocurrencies in Montenegro that are backed by the Government or the CBM.

Cryptocurrency regulation

Montenegrin legislation does not prohibit cryptocurrencies. That being said, only particular aspects of cryptocurrency relating to money transmission and anti-money laundering have been regulated so far in accordance with EU *acquis*. For more details, please see “Money transmission laws and anti-money laundering requirements” below.

Apart from those aspects related to money transmission and anti-money laundering, there is no relevant legislation regarding cryptocurrency in Montenegro. Currently, there is also no available practice pertaining to cryptocurrencies.

However, depending on the qualification of cryptocurrencies, i.e. whether they are treated as money, financial instruments or some other kind of assets, regulation applicable to those instruments/assets may apply to cryptocurrencies. Currently, there is no clear position on this matter (please see “Government attitude and definition” above).

The CBM has stated multiple times that, as a country in the process of EU accession, Montenegro will follow and implement solutions accepted within the Eurozone on this matter.

Sales regulation

There is no legislation regarding the sale of Bitcoins or other tokens in Montenegro.

However, depending on the qualification of cryptocurrencies, regulation applicable to certain instruments/assets may apply to cryptocurrencies. Currently, there is no clear position on this matter (please see “Government attitude and definition” above).

Taxation

Cryptocurrency is not subject to special tax law procedures in Montenegro. Accordingly, Montenegrin tax rules do not include any special tax rules for income, profits or gains arising from transactions involving cryptocurrencies.

The Tax Administration has not issued any official opinions about the tax regime applicable to certain transactions involving cryptocurrencies so far or the tax treatment of certain actions. There have been several transactions concerning the purchase and sale of immovable property in Montenegro using cryptocurrencies as a means of payment (in particular, Bitcoins). However, all such contracts contained a price in Euros in parallel. The Tax Authority of Montenegro applied taxes only on the corresponding value of the property expressed in Euros, and not in Bitcoins. Concerning these several cases, the Tax Authority explained that the trade of real estate, goods and services in Montenegro can be performed using virtual currencies, but that the corresponding value needs to be stated not only in Bitcoins but in the official currency as well in order to enable the calculation and collection of the value-added tax or real estate transfer tax.

Money transmission laws and anti-money laundering requirements

The AML Act has transposed some of the solutions provided for in Directive (EU) 2018/843 of the European Parliament and of the Council dated 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (please see “Government attitude and definition” above).

The AML Act explicitly lists legal entities and natural persons engaged in activities related to the issuing and managing of virtual currencies, including those providing exchange services between virtual currencies and conventional currencies as obliged entities which must implement measures for detecting and prevention of money laundering and terrorist financing.

The Rulebook on indicators for recognising suspicious clients and transactions (*Pravilnik o indikatorima za prepoznavanje sumnjivih klijenata i transakcija*) mentions the use of virtual currencies as terrorist financing indicators.

Promotion and testing

The CMC, in cooperation with the Ministry of Finance and the CBM, is currently considering the introduction of a blockchain and digital property market in Montenegro. Discussions have been held with the Chinese financial market authorities in this regard. The CMC has also organised multiple workshops on blockchain technology and its implementation.

CMC recently approved the creation of a regulatory Sandbox for two innovative ideas in providing financial services developed by Estonian companies: testing and development of global clearing and settlement based on the distributed ledger technology (“DLT”) network; as well as the digitisation of assets and development of a tokenised multilateral trading platform. The CMC is generally considered to be open to new initiatives in the area of blockchain and cryptocurrencies.

Ownership and licensing requirements

In Montenegro, there are no restrictions on investment managers owning cryptocurrencies for investment purposes, nor are there any explicit licensing requirements imposed on someone who holds cryptocurrency as an investment advisor or fund manager, apart from the general licensing requirements imposed on investment advisors/fund managers in accordance with capital markets regulations.

Mining

The mining of Bitcoins and other cryptocurrencies is also not regulated in Montenegro. Accordingly, it is not explicitly prohibited. However, there is a complete lack of regulatory framework and supervision over mining activities in Montenegro.

Border restrictions and declaration

There are no border restrictions nor obligations to declare cryptocurrency holdings. However, depending on the qualification of cryptocurrencies, border restrictions and declaration obligations applicable to certain instruments/assets may apply to cryptocurrencies. Currently, there is no clear position on this matter (please see “Government attitude and definition” above).

Reporting requirements

The AML Act prescribes that the obligation is to report transactions exceeding a value of EUR 15,000. Additionally, depending on the qualification of cryptocurrencies, reporting requirements applicable to certain instruments/assets may apply to cryptocurrencies. Currently, there is no clear position on this matter (please see “Government attitude and definition” above).

Estate planning and testamentary succession

There is no legislation, nor case law, confirming and explaining the use of cryptocurrencies for the purposes of estate planning and testamentary succession in Montenegro.



Jovan Barović

Tel: +381 60 3202 622 / Email: j.barovic@schoenherr.rs

Jovan Barović focuses on banking and finance as well as capital markets mandates in Serbia, Montenegro and North Macedonia. He has advised Joint Lead Managers on the issuance of Eurobonds by the Government of North Macedonia and the Government of Montenegro with a combined value of EUR 1 billion. He also advised Société Générale on the sale of its Montenegrin subsidiary through stock exchange transactions and takeover, and SBB in relation to the stock exchange acquisition of BBM. Jovan advises international banks regarding derivative and repo/reverse-repo transactions. Jovan's assignments include drafting the first ever Factoring Act for the Montenegrin Ministry of Finance, preparing amendments to the Montenegrin Financial Leasing Law, and drafting an expert report for the Serbian Government which analyses the existing key legal impediments to the sale of non-performing loans in Serbia.



Luka Veljović

Tel: +382 68 7376 87 / Email: l.veljovic@schoenherr.me

Luka Veljović is an associate who has been working with Schoenherr since 2018. Based in the Montenegro office, he is a member of the corporate/commercial practice group, with a track record in real estate and construction, energy and regulatory law in Montenegro and Serbia. He is engaged in corporate and regulatory matters in the construction, energy and financial services industries, and some of the clients he has advised include Shanghai Electric Power, Enemalta plc, Rakita Exploration, EPCG, Ludwig Pfeiffer, United Group and Adient Automotive. Luka graduated from the University of Montenegro, Faculty of Law, while spending part of his studies at the University of Maribor (Slovenia), the University of Zagreb (Croatia) and the University of Nice Sophia Antipolis (France).



Petar Vučinić

Tel: +382 67 7094 35 / Email: p.vucinic@schoenherr.me

Petar Vučinić is an associate who has been working with Schoenherr since 2018. Petar's main areas of practice are dispute resolution, banking, finance & capital markets and construction. He has experience in arbitration as well as in advising clients in bank insolvency proceedings and in the Montenegrin energy sector. Petar graduated from the Faculty of Law of the University of Montenegro in Podgorica (LL.B. 2018) where he also obtained a specialist diploma in business law (2019). Petar is fluent in English and German alongside his native Montenegrin language.

Moravčević Vojnović i Partneri AOD in cooperation with Schoenherr

Boulevard Džordža Vašingtona 98, The Capital Plaza, VIII floor, ME-81000 Podgorica, Montenegro

Tel: +382 20 228 137 / URL: www.schoenherr.eu

Portugal

Filipe Lowndes Marques & Mariana Albuquerque
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Government attitude and definition

Blockchain technology in general, and cryptocurrencies in particular, are closely followed topics in the financial technology industry amongst the Portuguese government and the relevant regulatory authorities, along with prevailing fintech trends in other jurisdictions. Particularly in recent years, these technologies have been brought to public attention largely due to the increase in the value of Bitcoin, the rise in the number of initial coin offerings (ICOs) globally, and their market capitalisation. This focus is also driven by some significant developments that the Portuguese market has seen in recent years in this sector, most notably the rise of tech-based companies and the steady increase in the use of cryptocurrencies in the last decade.

The most recent institutional developments include the approval of Ministerial Resolution 29/2020, dated 5 March 2020, which sets the framework principles for the creation of a Portuguese regulatory sandbox, and the approval of Ministerial Resolution 31/2020, dated 5 March 2020, which establishes the Portuguese Digital Mission Structure, which sets the main goals of the Portuguese digital agenda. The envisaged Portuguese regulatory sandbox should be overarching to include any area where technology should be given a freer testing field and will be designated by the terminology “Technology Free Zones” (from the Portuguese expression *Zonas Livres Tecnológicas*), and will be promoted and coordinated within the Portugal Digital Mission.

Blockchain technology is slowly being implemented in a significant number of projects in early stages of development, but is yet to have mainstream usage in private or public organisations. For these reasons, the government and regulatory authorities have been invested in studying blockchain technology and cryptocurrencies with a view to creating favourable conditions for the establishment and development of the sector, while protecting all market participants’ interests and also considering that there is a large base of Portuguese users participating in cryptocurrency transactions and/or investing in cryptocurrencies.

For the purpose of this chapter, cryptocurrencies can be broadly defined along the European Central Bank (ECB)’s definition – to which the Portuguese authorities have largely subscribed – as a “digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money”.¹ Other useful constructions have been developed by the European Securities and Markets Authority (ESMA) in its advice on ICOs and crypto-assets (January 2019)² and in a study requested by the European Parliament’s Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance (June 2018).³

In Portugal, cryptocurrencies do not have legal tender and thus do not qualify as fiat currency, nor are they treated as “money” (whether physical or scriptural) or, in principle,

“electronic money”. In this respect, the European Banking Authority (EBA) in its report of 9 January 2019⁴ has identified limited cases where cryptocurrencies can be considered “electronic money” as defined in Directive 2009/110/EC (EMD2), provided they match the criteria set in EMD2.

Nonetheless, cryptocurrencies are largely seen as an alternative payment method with a contractual nature that results from a private agreement between participants of cryptocurrency transactions, and with intrinsic characteristics that somewhat replicate some of the core traits of traditional money: storage of value; unit of account; and medium of exchange. Taking this into consideration, contrary to other countries that have been developing trials for government-backed cryptocurrencies, including those that have successfully launched government-backed cryptocurrency, there is no public governmental proposal to provide legal backing to cryptocurrencies. Cryptocurrencies are thus not backed by the Portuguese government or Banco de Portugal (Portugal’s central bank).

Cryptocurrencies can also be seen under a different light concerning their functionality. In this context, there has been recognition of other types of tokens, such as utility tokens and security tokens, commonly marketed through ICOs. These may be differentiated by their distinctive function, since the former are largely linked to consumption and the latter to investment. For this reason, they encompass or give rise to many other rights, including, among others, the right to receive a product or service or economic rights. In 2018, the Portuguese government actually issued a token – GOVTECH – which was used to cast votes by allocating those tokens to competing projects, thereby replicating investment choices, in a technological competition sponsored by the Portuguese government. The initiative was the first of its kind in Portugal and demonstrates the Portuguese government’s willingness to apply the technology (although still in a risk-free setting).

In light of the above, these new technologies have inevitably drawn the attention of the relevant regulatory authorities, most notably Banco de Portugal, the Portuguese securities authority (*Comissão do Mercado de Valores Mobiliários*, or CMVM) and the Portuguese insurance and pension funds authority (*Autoridade de Supervisão de Seguros e Fundos de Pensões*, or ASF).

Banco de Portugal, in its capacity as both central bank and national competent authority for the supervision of credit and payment institutions, has shown a clear interest in cryptocurrencies, notably from the perspective of consumer/investor protection, but has otherwise clarified that it will not take any immediate steps to regulate cryptocurrencies, having adopted instead a watchdog approach to the phenomenon and its development.

Nevertheless, since 2013, Banco de Portugal has issued a number of public statements and warnings in relation to cryptocurrencies, in line with the regulatory practices of other central banks of the eurozone and European regulatory authorities, such as the ECB and the EBA. We highlight, *inter alia*, Banco de Portugal’s publications that have included a warning focused on Bitcoin (November 2013), where it cited the ECB’s study, Virtual Currency Schemes (October 2012) (in which the ECB noted that it would be closely monitoring this phenomenon with a view to studying any necessary regulatory responses),⁵ and a warning to consumers regarding the potential risks in using cryptocurrencies (October 2014).⁶ Banco de Portugal has since also created a dedicated page headed “Virtual Currencies” on its website, where it warns consumers on the one hand, and credit institutions, payment institutions and electronic money institutions on the other hand, of certain risks entailed in cryptocurrencies.

In the same manner, the CMVM has published a warning to investors, in line with other European regulatory authorities such as ESMA, alerting them to the potential risks of

ICOs in order to raise awareness of these risks (November 2017),⁷ and has also issued a notice relating to a specific ICO for the issuance of Portuguese token Bityond (May 2018),⁸ stating that it did not consider it a security and, accordingly, Bityond was not subject to the CMVM's supervision or compliance with securities laws. A notice has also been issued to alert consumers to the risks of cryptocurrency (e.g. Bitcoin, Ether and Ripple), notably inadequate information and lack of transparency (July 2018).⁹

In 23 July 2018, the CMVM issued a formal notice addressed to all entities involved in ICOs¹⁰ regarding the legal qualification of tokens. The CMVM stressed the need for all entities involved in ICOs to assess the legal nature of the tokens being offered under the ICOs, in particular their possible qualification as securities with the application of securities laws as a consequence. In this context, the CMVM noted that tokens can represent very different rights and credits, and can be traded in organised markets, thus concluding that tokens can be qualified, on a case-by-case basis, as (atypical) securities under Portuguese law, most notably considering the broad definition of securities provided under the Portuguese Securities Code, approved by Decree-Law No. 486/99 of 13 November, as amended.

Notwithstanding, there still has not yet been any legislative impulse from either the Portuguese government or Parliament or from any other regulatory authority with specific laws or regulations in relation to cryptocurrencies, which therefore remain vastly unregulated from a systemic and teleological perspective.

Cryptocurrency regulation

As previously mentioned, at present there are no specific laws or regulations applicable to cryptocurrencies in Portugal, including in relation to their issuance and transfer. Hence, cryptocurrencies are not prohibited, and investors are allowed to purchase, hold and sell cryptocurrencies.

Nevertheless, on 10 March 2015, Banco de Portugal issued a recommendation, urging banks and other credit institutions, payment institutions and electronic money institutions, to abstain from buying, holding or selling virtual currency due to the risks associated with the use of virtual currency schemes identified by the EBA (the Bank of Portugal's Recommendation).¹¹

In relation to other types of tokens in Portugal, the same can be said as there are also no specific regulations applicable to other forms of virtual tokens.

However, one cannot say that there is a regulatory vacuum in this context, since existing laws will need to be assessed on a case-by-case basis to determine if they apply to a particular ICO, token or related activity. In this regard, the laws applicable to tokens will vary greatly depending on the specific characteristics of each token.

Thus, from a legal framework perspective, the main concern when analysing an ICO and the respective tokens will be to determine whether the ICO represents a utility token or a security token.

ICOs that aim to offer tokens that represent rights and/or economic interests in a specific project's results, use of software, access to certain platforms or virtual communities or other goods or services, may hypothetically overlap with consumer matters and become subject to certain regulations regarding consumer protection.

ICOs that aim to offer tokens that represent rights and/or economic interests in a pre-determined venture, project or company, such as tokens granting the holder a right to take

part in the profits of a venture, project or company or even currency-type tokens, may potentially be qualified as securities and cross over to securities' intensively regulated world, becoming subject to existing securities regulations, most notably regulations applicable to public offerings of securities and/or securities trading venues. In this respect, it should be noted that subsequent to ESMA's position in November 2017 stating that ICOs qualifying as financial instruments may be subject to regulation under EU law,¹² as of 9 January 2019, ESMA has published advice on ICOs and crypto-assets.¹³ Notably, under the heading "Regulatory implications when a crypto-asset qualifies as a financial instrument", ESMA provides advice on the potential application of, notably, the Prospectus Directive (Directive 2003/71/EC, as amended), the Transparency Directive (Directive 2013/50/EU), the Markets in Financial Instruments Directive (Directive 2014/65/EU), the Market in Financial Instruments Regulation (Regulation (EU) No. 600/2014) and respective implementing acts, the Market Abuse and Short-Selling Regulation (Regulation (EU) No. 596/2014 and Regulation (EU) No. 236/2012), the Settlement Finality Directive (Directive 2009/44/EC), the Central Securities Depository Regulation (Regulation (EU) No. 909/2014), and the Alternative Investment Fund Managers (AIFM) Directive (Directive 2011/61/EU).

It is also worth noting that, within the context of the information published regarding Portuguese cryptocurrency Bityond, mentioned above, the CMVM has already publicly stated that a token that allows its users to (i) participate in surveys related to the development of an online platform, and (ii) further donate tokens to the online platform for the development of new tools, is not qualified as a financial instrument, i.e. is not a security token, and therefore is not subject to securities law or the supervision of the CMVM.

Additionally, in its formal notice addressed to entities involved in ICOs, dated 23 July 2018, and mentioned above, the CMVM clarified the elements that may, in abstract, implicate the qualification of security tokens as securities, namely: (i) if they may be considered documents (whether in dematerialised or physical form) representative of one or more rights of a private and economic nature; and (ii) if, given their particular characteristics, they are similar to typical securities under Portuguese law. For the purpose of verifying the second item, the CMVM will take into account any elements, including those made available to potential investors (which may include any information documents, e.g. white paper), that may entail the issuer's obligation to undertake any actions from which the investor may draw an expectation to have a return on its investment, such as: (a) to grant the right to any type of income (e.g. the right to receive earnings or interest); or (b) undertaking certain actions, by the issuer or a related entity, aimed at increasing the token's value.

The CMVM thus concludes that if a token is qualified as a security and the respective ICO is addressed to Portuguese investors, the relevant national and EU laws shall apply, including, *inter alia*, those related to: the issuance, representation and transmission of securities; public offerings (if applicable); marketing of financial instruments for the purposes of MiFID II; information quality requirements; and market abuse rules. Finally, should the ICO qualify as a public offering, the CMVM further clarifies that a prospectus should be drafted and submitted, along with any marketing materials for the ICO, to the CMVM for approval, provided that no exemption applies in relation to the obligation to draw a prospectus. Lastly, in this notice, the CMVM also alerts that where a token does not qualify as a security, its issuer should avoid the use, including in the ICO's documentation, of any expressions that may be confused with expressions commonly used in the context of public offerings of securities, such as "investor", "investment", "secondary market" and "admission to trading".

Sales regulation

Considering the lack of exclusive regulation in relation to cryptocurrencies in Portugal, as described under “Cryptocurrency regulation” above, the purchase and sale of cryptocurrencies *per se* are also not specifically regulated.

However, to the extent that a token sale may be qualified as, for example, an offer of consumer goods or services or an offer of securities to the public, the relevant existing laws and regulations on, respectively, (i) consumer protection (including national laws that transposed, among others, Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services, Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market), and (ii) securities and financial markets (including national laws that transposed, among others, the Prospectus Directive, the Transparency Directive, MiFID II and the AIFM Directive), may apply by default, including their sanctions regime, subject to, in any case, an individual assessment. In these cases, both consumer protection law and securities law provide a number of obligations that must be complied with during and after the sale process. Therefore, existing regulations on the sale of consumers’ goods or services and of securities can apply to certain types of tokens on a case-by-case basis, in accordance with an “as-applicable principle”.

Taxation

In Portugal, there is no specific regime that deals exclusively with the taxation of cryptocurrencies. Nonetheless, the Portuguese Tax Authority has published three official rulings in the context of certain requests for binding information relating to cryptocurrencies: one in the context of personal income tax (December 2016);¹⁴ and the other two in the context of value-added tax (VAT) (January and July 2019).¹⁵ In the absence of other laws and regulations that may clarify the taxation regime of cryptocurrencies, these rulings have an important weight and will work as precedents in relation to how the Portuguese Tax Authority will look into cryptocurrency and cryptocurrency-related activities when interpreting existing tax provisions and deciding whether or not a certain fact or action should be subject to Portuguese tax (corporate, individual, VAT or stamp duty). In any event, as these were given in the context of requests for binding information, the Portuguese Tax Authority may revoke these rulings in the future.

In the 2016 official ruling, the Portuguese Tax Authority analysed the possible classification of cryptocurrencies within certain types of income that are subject to Portuguese tax, notably capital gains, capital income and income from business activities, and decided that, as a general rule, natural persons should not be taxed in respect of gains derived from the valuation or sale of cryptocurrencies, except that, in the case of sale of cryptocurrencies, if they correspond to the individual’s main recurrent activity, income obtained from such activity could be subject to Portuguese tax. It should also be noted that this was only a partial decision that did not elaborate on other types of income derived from other cryptocurrency-related activities (e.g. mining and farming activities).

In the 2019 official rulings, the Portuguese Tax Authority confirmed the precedent from the Court of Justice of the European Union (Case C-264/14, *Skatteverket v. David Hedqvist*) to argue that although cryptocurrencies such as Bitcoin were analogous to a “means of payment” and therefore subject to VAT, they were exempt by application of VAT exemption rules, which should be consistent across EU Member States considering existing VAT EU harmonisation.

Money transmission laws and anti-money laundering requirements

The Portuguese law on anti-money laundering and combatting terrorist financing¹⁶ (AML Law) imposes a general undertaking to obliged entities of risk management in the use of new technologies or products that are prone to favour anonymity.¹⁷ This means that, under Portuguese law, obliged entities are legally required to monitor the risks of money laundering and terrorist financing arising pursuant to the use of new technologies or developing technologies, whether for new products or existing ones,¹⁸ and, before launching any new products, processes or technologies, they will have to analyse any specific risks of money laundering or terrorist financing related to it, and to document the specific procedures adopted for their risk mitigation.

In addition, obliged entities must undertake identification procedures and customer due diligence whenever there is an occasional transaction of more than €15,000, as well as reinforce their identification procedures and customer due diligence when they identify an additional risk of money laundering or terrorist financing in business relationships, in occasional transactions or in the usual operations of the customer. Pursuant to the AML Law, an additional risk is presumed to exist in products or operations that favour anonymity, in new products or commercial activities, in new distribution mechanisms and payment methods, and in the use of new technologies or developing technologies, whether for new products or existing ones. This has obvious implications for cryptocurrencies and cryptocurrency-related activities (including cryptocurrency exchanges) in case those operations intersect with the activities and operations of entities that are covered by obligations imposed by anti-money laundering and combatting terrorist financing, since obliged entities should reinforce their identification procedures and customer due diligence when participating in any related operation.

In the banking sector, the Bank of Portugal's Recommendation, mentioned above, was also driven by concerns of the risks of money laundering, terrorist financing and other financial crime arising pursuant to the overall predominance of anonymity and lack of intermediaries that would communicate suspicious activities to the authorities.¹⁹ This Recommendation followed a previous warning to consumers issued in October 2014, as mentioned above, that was made in response to the fact that certain automated teller machines (ATMs) in Portugal, which were not integrated in the Portuguese payment system, were enabling exchange between Bitcoin and euros.

Banco de Portugal's stance in respect of cryptocurrencies does not affect other market participants such as consumers, investors and other entities that wish to, respectively, hold, invest or develop cryptocurrencies; however, it goes a long way towards reducing the participation of banks and other credit institutions, payment institutions, and electronic money institutions that are traditional "obliged entities" for the purposes of anti-money laundering and combatting terrorist financing laws. It should also be noted that insofar as operations in cryptocurrencies are not undertaken by obliged entities (as legally defined), compliance with and enforcement of anti-money laundering and terrorist financing laws should be diluted, as cryptocurrencies and related activities are confined to virtual platforms and private relations.

Furthermore, considering the deadline for the transposition of the fifth Anti-Money Laundering Directive (AMLD 5),²⁰ additional obligations in relation to cryptocurrency exchanges and custodian wallet providers are expected to come into force soon. The transposition deadline of AMLD 5 was 10 January 2020, and there is currently a legislative proposal in the Portuguese Parliament for the transposition of this legal act. The proposal introduces a legal concept of "virtual asset" that encompasses the digital representation of

value that is not necessarily linked to a legally established currency and that does not have the legal status of fiat currency, but which is accepted by natural or legal persons as a means of exchange or of investment and which can be transferred, stored and traded electronically. If approved, the new legal act establishes – as expected – that cryptocurrency exchanges that accept fiat currency and custodian wallet providers will become subject to the AML Law. Furthermore, this proposal foresees that these entities must register with Banco de Portugal.

Promotion and testing

The Portuguese government had initially launched a think tank with the objective of generally promoting and fostering fintech – mostly by identifying and targeting entry barriers – with the ultimate aim to implement a regulatory “sandbox” with the aid of the Portuguese financial regulators. Now, with the publication of the Ministerial Resolutions referred to above and the creation of the Portuguese Digital Mission Structure, the launch of a Portuguese regulatory sandbox is closer to being achieved.

Additionally, both the CMVM and Banco de Portugal have specific spaces for fintech on their webpages, <http://www.cmvm.pt/en/> and <https://www.bportugal.pt/en/>, respectively, which include, *inter alia*, information regarding distributed ledger technology, ICOs, and tokens.

These fintech spaces were created with the intent to facilitate the provision and exchange of information and dialogue between these regulators and developers or sponsors of new financial technologies that cross over with the areas of regulatory competence of the CMVM and Banco de Portugal, and also to clarify the regulatory framework applicable to the same. These objectives are obtained mainly by having a dedicated contact within the CMVM and Banco de Portugal that deals solely with issues relating to fintech, and by being active in promoting conferences and workshops aimed at investors and the public in general with a formative and educational goal.

In 2018, a non-profit organisation, Portugal Fintech, and Banco de Portugal, the CMVM and ASF, joined efforts to create “Portugal FinLab – where regulation meets innovation”, which created a direct communication platform for emerging tech companies working in fintech-related subjects, incumbents and Portuguese regulators to engage and to provide guidance on a more clear path of action in terms of the application of the existing regulatory framework to the activities of those companies. Portugal Fintech also manages the Portugal Fintech Report, which is an annual report that contains data regarding the Portuguese fintech ecosystem and its development, and the Fintech House, launched in January 2020, which is a fintech hub.

Ownership and licensing requirements

As mentioned in “Cryptocurrency regulation” above, in Portugal, there are no specific restrictions or licensing requirements when it comes to purchasing, holding or selling cryptocurrencies from the user’s perspective (for cryptocurrency businesses we note that this will change slightly as a result of the transposition of AMLD 5 into Portuguese legislation), except where they are qualified as securities.

Furthermore, insofar as cryptocurrencies are not qualified as financial instruments, advisory services that are made exclusively in relation to, and the exclusive management of, cryptocurrency portfolios are not subject to the same investment services laws and regulations as those applicable to securities. Thus, these types of activities, when undertaken solely in relation to cryptocurrencies, are not subject to any licensing requirements.

However, traditional advisory services and management services require licensing and are subject to the CMVM’s supervision.

One thing to note is that, given the fact that these instruments are not yet mainstream for consumers, the overall regulatory uncertainty and even some regulatory pushback (e.g. the Bank of Portugal's Recommendation), underpinned by the already existing and overarching obligations applicable to the provision of investment services, it is not likely for the time being that traditional investment advisors, including, among others, credit institutions and fund managers, will recommend or invest in cryptocurrencies.

Mining

There are no restrictions in Portugal on the development of mining of cryptocurrencies and the activity itself is not regulated.

Border restrictions and declaration

In Portugal, there are no border restrictions or obligations to declare cryptocurrency holdings.

Reporting requirements

There is no standalone reporting obligation in case of cryptocurrency payments above a certain threshold, except in the case of transactions that may involve an obliged entity covered by anti-money laundering and terrorist financing laws, in which case such entity will have to report suspicious transactions or activities irrespective of the amounts involved.

Estate planning and testamentary succession

There is no precedent, specific rules or particular approach regarding the treatment of cryptocurrencies for the purposes of estate planning and testamentary succession in Portugal. Notwithstanding, certain aspects of estate planning and testamentary succession should be highlighted. Inheritance tax does not exist in Portugal, but stamp duty may apply to certain transfers of certain assets (e.g. immovable property, movable assets, securities and negotiable instruments, provided they are located, or deemed to be located, in Portugal) included in the deceased's estate in case of succession.

However, in the absence of a legal amendment or binding information from the Portuguese tax authorities, it may be argued that the drafting of the relevant legal provisions does not expressly foresee assets such as cryptocurrencies, thus excluding the same from the scope of application of stamp duty, which *de facto* mitigates the need for estate planning with respect to cryptocurrencies. Estate planning and testamentary succession must therefore be analysed on a case-by-case basis, considering all variables involved.

* * *

Endnotes

1. *Cf.* EUROPEAN CENTRAL BANK, Virtual currency schemes – a further analysis, February 2015, available at <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>. See also the definition of virtual currency included in the fifth AML Directive (Directive (EU) 2018/843).
2. *Cf.* EUROPEAN SECURITIES AND MARKETS AUTHORITY, “Advice: Initial Coin Offerings and Crypto-Assets”, dated 9 January 2019, available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
3. *Cf.* ROBBY HOUBEN, ALEXANDER SNYERS, “Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion”,

- study at the request of the European Parliament’s Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance, dated June 2018, available at <http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>.
4. *Cf.* EUROPEAN BANKING AUTHORITY, EBA Report with advice for the European Commission on crypto-assets, 9 January 2019, available at <https://eba.europa.eu/>.
 5. *Cf.* BANCO DE PORTUGAL’s public statement regarding Bitcoin, dated 22 November 2013, available in Portuguese at <https://www.bportugal.pt/comunicado/esclarecimento-do-banco-de-portugal-sobre-bitcoin>.
 6. *Cf.* BANCO DE PORTUGAL’s warning regarding the risks associated with cryptocurrencies, dated 3 October 2014, available in Portuguese at <https://www.bportugal.pt/comunicado/alerta-aos-consumidores-para-os-riscos-de-utilizacao-de-moedas-virtuais>.
 7. *Cf.* CMVM’s warning regarding the risks associated with ICOs, dated 3 November 2017, available in English at <http://www.cmvm.pt/en/Comunicados/Comunicados/Pages/20180119.aspx>.
 8. *Cf.* CMVM’s notice regarding the cryptocurrency Bityond, dated 17 May 2018, available in Portuguese at <http://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20180517a.aspx>.
 9. *Cf.* CMVM’s notice regarding risks of “virtual currencies”, dated 5 July 2018, available in Portuguese at <http://www.cmvm.pt/pt/CMVM/CNSF/ConselhoNacionalDeSupervisoresFinanceiros/Pages/20180705.aspx>.
 10. CMVM’s notice addressed to all entities involved in ICOs, dated 23 July 2018, available in Portuguese at <http://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20180723a.aspx?v=>.
 11. *Cf.* BANCO DE PORTUGAL’s Circular Letter No. 11/2015/DPG, dated 10 March 2015, Recommendation relating to buying, holding and selling virtual currencies, available in Portuguese at <https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/11-2015-dpg.pdf>.
 12. *Cf.* EUROPEAN SECURITIES AND MARKETS AUTHORITY, Statement “ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements”, dated 13 November 2017, available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.
 13. See endnote 2 above.
 14. *Cf.* AUTORIDADE TRIBUTÁRIA E ADUANEIRA, Binding Information provided in process No. 5717/2015, dated 27 December 2016.
 15. *Cf.* AUTORIDADE TRIBUTÁRIA E ADUANEIRA, Binding Information provided in process No. 14763, dated 28 January 2019 and in process No. 14436, dated 3 July 2019.
 16. Law No. 83/2017, of 18 August, transposing Directives 2015/849/EU of the European Parliament and of the Council of May 20, and 2016/2258/EU of the Council of 6 December.
 17. *Cf.* Article 15 of Law No. 83/2017.
 18. *Cf.* Article 36 (5) and Annex III of Law No. 83/2017.
 19. *Cf.* EUROPEAN BANKING AUTHORITY, EBA Opinion on “virtual currencies” (EBA/Op/2014/08), 4 July 2014, available at <https://www.eba.europa.eu/>.
 20. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

**Filipe Lowndes Marques****Tel: +351 213 817 400 / Email: flmarques@mlgts.pt**

Filipe Lowndes Marques joined the firm in 2001. He is the coordinator of the banking and finance department and the restructuring and insolvency department.

Filipe has worked since 1995 in the area of loan and bond finance, representing lenders and borrowers, including restructurings of existing financings. In the project finance sector, he has worked on several types of project, including bridges, motorways, power plants, wind and solar farms, football stadia, LNG terminals and natural gas concessions.

He has also been active in the field of capital markets, having advised on several securitisation transactions (including the first securitisation transaction under the new law and the first synthetic securitisation) and covered bonds issuances and working on several IPOs of state-owned companies.

His investment fund team was considered by *Chambers Europe* as “Portugal’s top practice in investment funds”.

**Mariana Albuquerque****Tel: +351 213 817 400 / Email: msalbuquerque@mlgts.pt**

Mariana Albuquerque joined the firm in 2014. She is a member of the banking and finance team and of Team Genesis.

She develops her work primarily in the area of banking and finance law, with a special focus on compliance by providing legal advice and consultancy with regard to the regulation and supervision of banks and other financial institutions, in payment services, in securitisation transactions, in negotiating derivatives and other financial instruments, in structured finance, in corporate finance and in project finance transactions.

As a member of Team Genesis, Mariana works primarily with Fintech- and Regtech-related subjects.

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Rua Castilho, 165, 1070-050 Lisbon, Portugal

Tel: +351 213 817 400 / URL: www.mlgts.pt

Serbia

Bojan Rajić & Mina Mihaljčić
Moravčević Vojnović i Partneri AOD Beograd
in cooperation with Schoenherr

Government attitude and definition

In March 2019, the Securities Commission of Serbia (“Commission”) issued a Statement on the regulation of crypto-assets in the Republic of Serbia (“Statement”), under which the Commission, in cooperation with the Office of the Prime Minister, launched a public consultation process on the regulation of crypto-assets in Serbia. Here it should be noted that although the Statement is not considered an official opinion of the Commission, we may look at it as a reflection of its current understanding and position on the matter.

Since there is a lack of clarity as to how the Serbian regulatory framework applies to crypto-assets, such instruments raise specific challenges for regulators and market participants. The Commission’s current position is that the development of crypto-assets does not currently raise financial stability issues. Such opinion is in line with the paper issued by the European Securities and Market Authority (“ESMA”) in its Advice Paper (*Initial Coins Offerings and Crypto-Assets*), issued on 9 January 2019. Also, the Commission has noted that the IT industry in Serbia is on the rise and in order to support the development of the industry, it is necessary to ensure legal certainty. The Commission believes that this could be achieved by establishing the competent institutions regarding crypto-assets, but also by application of the existing regulations where appropriate. However, there is also a concern about the risks that could affect the Serbian market or prospective investors.

In its Statement, the Commission outlined its position on the gaps and issues that exist in the rules in situations when crypto-assets qualify as financial instruments and the risks that can arise when crypto-assets do not qualify as financial instruments.

The Commission believes that crypto-assets that can be qualified as one of the financial instruments under Article 2(1) of the Capital Markets Act (*RS Official Gazette, nos 31/2011, 112/2015, 108/2016 and 9/2020 (subsequent amendment)*) (“CMA”) are regulated by Serbian law and fall within the Commission’s remit.

Accordingly, the Commission defines the criteria for determining whether a crypto-asset could be qualified as a financial instrument or not. Taking into account the definition of *transferable securities* as defined in the CMA, a crypto-asset would have the features of a transferable security if it were: (i) not used for purchasing goods and services; (ii) negotiable on the capital market; and (iii) to include at least one of the following: (A) right to a participation in the issuer’s capital or voting rights; (B) right to register the rights defined under item (A) with the relevant public register; (C) right to receive remaining assets (liquidation proceedings); (D) right to a claim from the issuer determined as a fixed sum with a maturity of more than 397 days from the day of issue; (E) right to register the rights defined under item (D) with the relevant public register; (F) right to acquire securities;

and/or (G) right to a claim from the issuer determined by reference to transferable securities, currencies, interest rates, incomes, commodities, indices or other measures.

The Commission's preliminary view is that where crypto-assets qualify as financial instruments, the regulatory framework stipulated by the CMA should apply to them and to all transactions with respect to the crypto-assets. In such case, the provisions on prospectuses, reporting and rules on secondary trading must be applied as well. So, IT companies dealing with such crypto-assets must satisfy all provided conditions and obligations required for issuers of financial instruments. This is particularly applicable to so-called "investment tokens", i.e. digital tokens with an investment/speculative purpose, which are considered already regulated financial instruments issued in the new form, through new blockchain technology.

On the other hand, in cases where crypto-assets do not qualify as financial instruments, the Commission took the position that the existing Serbian legislation cannot be applied directly. The legal framework proposed by the Commission for this type of crypto-asset is similar to the system for issuing and trading in financial instruments established by the CMA and European Union directives. Here, the Commission believes that Serbia has an opportunity to adopt a straightforward regulatory framework – which could have a positive impact on the development of the IT sector.

In this regard, the Commission has proposed the following significant features of the prospective legal framework:

- the Commission would license agents providing professional services with respect to crypto-assets, and the issuers of crypto-assets would be required to conclude an agreement with such agent. Also, the agents would provide advice to issuers in relation to their obligations, represent them before the regulatory authority and file the required reports with the regulatory authority, etc. The agents would have an important role in the prevention of money laundering and terrorism financing;
- the issuer should publish a whitepaper at least 10 days before a crypto-asset has been issued. The whitepaper would be signed by management members of an issuer and would contain the prescribed information. These documents should be similar to a prospectus regulated under the CMA regarding securities, only simpler; and
- anyone who intends to provide services in relation to issuing/trading in crypto-assets will be required to hold a licence issued by the Commission. The services include organisation of trading, receipt and execution of orders, custody services, providing investment advice, portfolio management, etc.

The above overview of the prospective legal framework is not exhaustive, but rather highlights some of its key features.

In a separate instance, the Serbian central bank – the National Bank of Serbia ("NBS") – took a position on whether cryptocurrencies can be considered currencies. Namely, on 3 November 2017, NBS issued an official opinion on cryptocurrencies pursuant to which it confirmed that cryptocurrencies are not considered currencies under Serbian law. Accordingly, trading of cryptocurrencies and platforms for internet trading of cryptocurrencies are not subject to NBS supervision. The exceptions to this are matters regarding anti-money laundering regulations, where NBS explicitly recognises its supervising authority (please see "Money transmission laws and anti-money laundering requirements" below).

NBS further emphasised its concern about the risks Bitcoin poses to cryptocurrency users, and also issued a separate warning stating that anyone involved in virtual currency activities is doing so on their own responsibility, bearing their own financial risk.

Cryptocurrency regulation

While Serbian law does not prohibit cryptocurrencies, there is currently no specific legislation applicable to cryptocurrencies either. However, in the last two years, different proposals for governing cryptocurrencies and related matters have been published (please see “Government attitude and definition” above).

Sales regulation

In cases where cryptocurrencies can be qualified as financial instruments (for details, please see “Government attitude and definition” above), the provisions of the CMA must be applied to the sale process. On the other hand, in cases where cryptocurrencies do not qualify as financial instruments, the general civil law rules (particularly the Serbian Obligation Act) would apply.

However, it should be noted that, at this time, cryptocurrencies have not yet been explicitly qualified as securities, nor are they subject to the CMA.

Taxation

Serbia has not enacted any specific tax regulation concerning cryptocurrencies. Accordingly, Serbian tax rules do not include any special tax rules for income, profits or gains arising from transactions involving cryptocurrencies.

So far, the Serbian Ministry of Finance has issued only one opinion on cryptocurrencies, following the opinion of NBS, pursuant to which cryptocurrencies, and in particular Bitcoin, are not considered currencies under Serbian law (referred to under “Government attitude and definition” above).

Following the opinion given by NBS, on 26 November 2017, the Ministry of Finance of the Republic of Serbia issued its opinion no. 413-00-168/2017-04, referring to Article 25(1)1) of the Value-Added Tax Act (*RS Official Gazette, nos 84/2004, 86/2004, 61/2005, 61/2007, 93/12, 108/13, 68/14, 142/14, 83/15, 108/16, 13/17, 30/18, 72/19 and 8/20*), which prescribes a tax exemption without the right to deduct input VAT on transactions concerning legal means of payment (legal tender), which cannot be applied to the trade of Bitcoin, as Bitcoin does not represent a form of legal payment in Serbia. Hence, the sale of cryptocurrencies is not subject to VAT in Serbia.

When considering whether cryptocurrencies are subject to income tax, the situation is not clear-cut. Namely, the Individual Income Tax Act does not specify cryptocurrencies as a revenue source subject to income tax. However, the mentioned Act contains a general provision pursuant to which “other revenues” subject to income tax can be “all other revenues not subject to taxes on the basis of other laws or which are not freed from taxes or free from paying taxes on the basis of the Act”. Consequently, it should be considered that income arising from the sale of cryptocurrencies, just as that arising from the sale of other assets, can be considered subject to personal income tax (which would in this case be 20%).

Money transmission laws and anti-money laundering requirements

Although crypto-assets are not regulated in the Serbian legal system, provisions of the Law on Prevention of Money Laundering and Terrorism Financing (*RS Official Gazette, nos 113/2017 and 91/2019*) (“AML Act”) already cover crypto-assets to a significant extent; i.e. there are grounds for interpretation of the current rules to be applicable to crypto-assets, as it explicitly recognises the term “virtual currencies”.

Also, the Serbian Criminal Code (*RS Official Gazette, nos 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019*) (“Criminal Code”) sanctions the crime of money laundering. Namely, under the Criminal Code:

“The one who converts or transfers assets while aware that such assets originate from a criminal activity, with intent to conceal or misrepresent the unlawful origin of the assets, or conceals and misrepresents facts on the assets while aware that such assets originate from a criminal activity, or obtains, keeps or uses assets with the intent, at the moment of receiving, that such assets originate from a criminal activity, shall be punished by imprisonment of six months to five years and a fine.”

The Commission believes that the term “asset” can be interpreted to include crypto-assets, so the Criminal Code regulates laundering of crypto-assets as a criminal activity as described. Additionally, the AML Act stipulates that NBS supervises legal persons and individuals that provide services in relation to virtual currencies. The most recent update in AML regulations in Serbia was made by the latest amendments to the AML Act (December 2019). These amendments introduced a new set of rules aiming to regulate prevention of money laundering and terrorism financing in more detail, also introducing the term “virtual currency”. A virtual currency is defined as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat (conventional) currency and does not have legal tender status, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.

Promotion and testing

At the time of writing, we are not aware of any public “sandbox” or other programmes aimed at specifically promoting research or investment into cryptocurrencies in Serbia. However, there are various initiatives in the private sector in Serbia that directly or indirectly promote blockchain technologies.

Ownership and licensing requirements

If cryptocurrencies are used as financial instruments, they will be subject to stock market regulation. At the time of writing, there are no specific licensing requirements imposed on an investment advisor or fund manager holding cryptocurrencies.

Mining

Mining of cryptocurrencies is not subject to regulation in Serbia. It is not prohibited as such; however, there are no rules that regulate under which conditions and how mining activities can be undertaken. It can hence be deduced that mining is currently permitted in Serbia. Also, no authority has yet assumed the mining of cryptocurrencies as falling under its (explicit) supervision.

Publicly available information and media reports suggest that mining activities are indeed undertaken in Serbia, although they do not appear to be widespread.

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings under Serbian law.

Reporting requirements

There are currently no specific reporting requirements aimed at cryptocurrency payments made in excess of a certain value under Serbian law.

However, it should be presumed that general AML rules may also be applicable to cryptocurrency and blockchain transactions, i.e. that certain AML requirements apply irrespective of the transaction being made in cryptocurrencies or via blockchain (e.g. identification and reporting of activities suspected of money laundering or terrorism financing).

Estate planning and testamentary succession

There are no specific rules as to how cryptocurrencies are treated for purposes of estate planning and testamentary succession.

Even though cryptocurrencies are not explicitly subject to civil law in Serbia, cryptocurrencies could be qualified as intangible assets from a Serbian civil law perspective. As such, they do not differ from ordinary assets and can be included in estate planning and testamentary succession.

**Bojan Rajić****Tel: +381 60 320 26 32 / Email: b.rajic@schoenherr.rs**

Bojan Rajić specialises in corporate/M&A and employment. Bojan advises international clients on their market entry and is a member of the team that provides full-service transactional support in the implementation of their investments. He is a specialist of contracts and investments incentives. He advised on the sale of IT start-up 3Lateral to Epic Games, Smurfit Kappa Group on the acquisition of the largest integrated packaging business in Serbia, and Telenor on the sale of its subsidiary in Serbia. He advised Adient Seating on the establishment of a new plant in Serbia, including in relation to relevant subsidies and negotiations of the corresponding grants agreement. Recently, Bojan acted as legal counsel and provided all M&A, regulatory and general corporate services to Solelos (former GameCredits), an IT company operating various blockchain-based and cryptocurrency projects.

**Mina Mihaljčić****Tel: +381 60 320 26 20 / Email: m.mihaljcic@schoenherr.rs**

Mina Mihaljčić has been an associate with the firm since 2017. She specialises in corporate/M&A. She has advised clients in the IT, telecommunications, banking and finance and packaging industries. Most recently she advised on the sale of an innovative technologies developer from Serbia to Epic Games and the leading telecom operator on the acquisition of a major cable television, broadband internet and mobile service provider. Mina acted as legal counsel and provided all M&A, regulatory and general corporate services to Solelos (formerly GameCredits), an IT company operating various blockchain-based and cryptocurrency projects.

Moravčević Vojnović i Partneri AOD Beograd in cooperation with Schoenherr

Bulevar vojvode Bojovića 6–8, 11000 Belgrade, Serbia

Tel: +381 11 320 26 00 / URL: www.schoenherr.rs

Switzerland

Daniel Haeberli, Stefan Oesterhelt & Alexander Wherlock
Homburger AG

Government attitude and definition

Introduction

In Switzerland, the government's general attitude towards cryptocurrencies, and in particular towards the technology underlying cryptocurrencies, is very positive.

Both the Swiss federal government as well as the Swiss Financial Market Supervisory Authority (“**FINMA**”) recognise the potential that blockchain and distributed ledger technology (“**DLT**”) offer to the financial services industry as well as various other areas of the economy. Switzerland sees an opportunity to take a global lead in this sector, and officials and authorities are generally open *vis-à-vis* new developments. This is particularly true for cantonal, *i.e.*, state, authorities, namely in the Canton of Zug.

In December 2018, the Swiss Federal Council published a comprehensive report covering the legal framework for DLT and blockchain in Switzerland.¹ The report generally concluded that Switzerland's current legal framework, in principle, already provides for adequate regulations, covering the questions arising in connection with the development of new technologies, such as DLT. However, a need for selective action and improvements in certain areas of private, financial market and insolvency law was identified. In light of these findings, the Swiss Federal Council published a draft law relating to blockchain and DLT (“**DLT-Draft Law**”) on March 22, 2019² as well as the dispatch to the DLT-Draft Law (“**Dispatch**”) on November 27, 2019.³ The Swiss Federal Council, the Swiss Federal National Council, as well as the Economic Affairs and Taxation Committee of the Swiss Federal Council of States, approved the DLT-Draft Law after making some minor changes to the draft. It is expected that the Swiss Federal Council of States will deliberate on the adjusted DLT-Draft Law in its 2020 autumn session.

Definition

Swiss law does not define the term cryptocurrency or virtual currency. However, the Swiss federal government had to address the topic of virtual currencies in a special report dated June 25, 2014.⁴ In this report, the following definition was used:

“A virtual currency is a digital representation of a value which can be traded on the Internet and although it takes on the role of money – it can be used as means of payment for real goods and services – it is not accepted as legal tender anywhere. (...) Virtual currencies exist only as a digital code and therefore do not have a physical counterpart for example in the form of coins or notes. Given their tradability, virtual currencies should be classified as an asset.”

The same definition was later used by FINMA, when the relevant anti-money laundering regulations were amended,⁵ and the term virtual currency is also mentioned in the Swiss anti-money laundering ordinance (“AMLO”) since January 1, 2016.⁶

However, given that there is no statutory definition and no case law, currently the best approach is to rely on the token categories introduced by FINMA in its “Guidelines for enquiries regarding the regulatory framework for initial coin offerings” (“ICOs”) (“**FINMA ICO Guidelines**”) of February 2018.⁷ Based on this classification, which is also referenced and used by the Swiss Federal Council in the Dispatch,⁸ the following three categories of tokens can be distinguished:

- Payment tokens (which are, according to FINMA, synonymous with “pure cryptocurrencies”; referred to herein as “cryptocurrencies”) are tokens that are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Pure “cryptocurrencies” do not give rise to any claims towards an issuer or a third party. Consequently, according to the prevailing view, these tokens are “purely factual intangible assets”.⁹ Examples of such cryptocurrencies are Bitcoin (including numerous cryptocurrencies resulting from forks or variations of Bitcoin, such as Bitcoin Cash, Bitcoin Gold and Litecoin) and Ether.
- Utility tokens are tokens that are intended to provide access digitally to an application or service by means of a DLT-based infrastructure.
- Asset tokens represent assets such as a debt or an equity claim against the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, such tokens are analogous to equities, bonds or derivatives. Tokens, which enable physical assets to be traded on a blockchain infrastructure, according to FINMA, also fall into this category.

FINMA points out that tokens may also fall into more than one of these three basic categories. Such *hybrid tokens* are, for example, asset tokens or utility tokens, which at the same time also qualify as payment tokens.

Moreover, FINMA published a supplement to the FINMA ICO Guidelines (“**FINMA Supplement**”) on September 11, 2019¹⁰ as an answer to an increase of regulatory enquiries in relation to crypto projects using so-called “stable coins”. Generally, a stable coin is a token whose value is derived from an underlying asset that is considered stable, in order to limit the volatility of the token’s price.¹¹ Such a token can, for example, be linked to an individual or a basket of currencies, real estate, securities or commodities. Examples of such stable coins are Tether, True USD or Digix DAO.¹² However, other types of stable coins use stabilisation mechanisms without a direct linkage to any underlying or collateral, as the case may be. Although a number of variations exist, such coins use algorithms or other (automated) systems to stabilise the price of the token by directly or indirectly influencing the demand and supply of the respective token. For example, depending on the current price of the respective token, more tokens may be issued or bought back from the market.¹³

Cryptocurrencies are not legal tender

In Switzerland, cryptocurrencies do not qualify as legal tender.¹⁴ Consequently, cryptocurrencies are not considered “money” in a narrow sense. However, some legal scholars argue that cryptocurrencies, provided they are widely used, are accepted by the public and have adopted the typical functions of money, qualify as “money” in a broader sense.¹⁵ The Swiss Federal Council, however, does not seem to follow this view.¹⁶

Also, there is currently no form of “state-backed” cryptocurrency available in Switzerland. In particular, the Swiss National Bank, Switzerland’s central bank, has not issued any

cryptocurrencies, nor are there any concrete indications that it intends to do so in the near future.¹⁷ However, on October 8, 2019, the Swiss National Bank entered into an operational agreement with the Bank for International Settlements (“**BIS**”) regarding the BIS Innovation Hub Centre located in Switzerland. The aim of this Innovation Hub is to gain in-depth knowledge of the relevant technological developments affecting the tasks of central banks. In one of the research projects under this initiative, the integration of digital central bank money into a DLT infrastructure is being tested. This new form of digital central bank money may allow the settlement of “tokenised” assets between financial institutions. The project is being implemented in the form of a feasibility study as part of a cooperation between the Swiss National Bank and the SIX Group.¹⁸

Moreover, tax authorities in the Canton of Zug will start accepting Bitcoin and Ether for tax payments as of 2021. Thus, the Canton of Zug will be the first Swiss canton in which taxes can be paid with cryptocurrencies.¹⁹

The Swiss Federal Council’s recent legislative initiative

The DLT-Draft Law suggests the introduction of a new concept of so-called “DLT-Rights”, allowing for the tokenisation of rights, claims and financial instruments, such as bonds, shares or derivatives. The concept of DLT-Rights aims to ensure the tokenisation of rights by providing the legal framework for an electronic registration of rights that entails the same protection as a negotiable security.

Contractual claims (namely under a bond or other debt instruments) or certain membership rights (e.g., shares in a corporation) both qualify as an admissible underlying of a DLT-Right.²⁰ Therefore, in particular, asset tokens, such as certain types of stable coins and certain types of utility tokens, could be issued as DLT-Rights under the DLT-Draft Law.²¹ On the other hand, cryptocurrencies (such as, for example, Bitcoin or certain types of stable coins) that do not give rise to a claim against an issuer and therefore do not have an admissible underlying within the meaning of the DLT-Draft Law, cannot be issued in the form of DLT-Rights.²²

After having been revised and approved by the Swiss Federal National Council and the Economic Affairs and Taxation Committee of the Swiss Federal Council of States, it is expected that the Swiss Federal Council of States will deliberate on the adjusted DLT-Draft Law in its 2020 autumn session. It is therefore still unclear whether any additional amendments will be made to the draft by the Swiss Federal Council of States and when the DLT-Draft Law will enter into force.

Cryptocurrency legislation

In Switzerland, cryptocurrency-related activities are not prohibited. Further, subject to the enactment of the DLT-Draft Law, there are currently (apart from the provision in the AMLO mentioned under “Government attitude and definition”, above) no Swiss statutes or regulations that are tailor-made for cryptocurrencies.

Sales regulation

While offering and selling cryptocurrencies is not subject to specific Swiss sales regulations, an offer and sale of utility tokens, asset tokens and stable coins may become subject to offer/sales regulations if the tokens in question constitute securities within the meaning of Swiss law. Under Swiss law, securities (*Effekten*) are financial instruments, which are: (i) standardised; (ii) suitable for mass trading; and (iii) either certificated securities (*Wertpapiere*), uncertificated

securities (*Wertrechte*), derivatives or intermediated securities (*Bucheffekten*).²³ Whether, or which, tokens are securities is currently not entirely clear, *i.e.*, there is neither any statutory guidance nor any case law regarding this question. Therefore, each token will have to be subject to a specific determination on a case-by-case basis in consideration of the principles outlined by FINMA.

However, in its ICO Guidelines (see above, “Definition”), FINMA indicated that, generally speaking, it does not intend to qualify cryptocurrencies as securities. According to FINMA, utility tokens are not treated as securities if their sole purpose is to confer digital access rights to an application or service, and if the utility tokens can already be used in this way at the point of issue. This view on payment and utility tokens is supported by the Dispatch.²⁴

Currently,²⁵ FINMA has the following view on whether tokens qualify as securities or not:²⁶

- Cryptocurrencies to date are not treated as securities by FINMA. In our opinion, this assessment is correct. Cryptocurrencies do not grant their holders or users any relative or absolute rights *vis-à-vis* an issuer or a third party. They serve as mediums of exchange and (arguably) also as units of account and storage of value. Whether cryptocurrencies are “financial instruments” as defined in the recently adopted Swiss Financial Services Act (“**FinSA**”),²⁷ which entered into force on January 1, 2020, remains unclear. Given the wording of the FinSA, we are of the opinion that cryptocurrencies are not “financial instruments” within the meaning of the cited Act (see below, “Securities firm licence”).
- Utility tokens are currently not treated as securities by FINMA, provided that: (i) their sole purpose is to confer digital access rights to an application or service; and (ii) the tokens can actually already be used in this manner when they are issued. If these two conditions are met, the typical “connection with capital markets” inherent to securities, according to FINMA, does not exist. FINMA points out that it will qualify utility tokens as securities if they fully or partially “have the economic function of an investment”.
- Asset tokens shall, according to FINMA, generally be treated as securities; for example, if they represent uncertified securities or derivatives and are standardised as well as suitable for mass trading. As FINMA points out, uncertificated securities may also be created in so-called pre-financing and pre-sale scenarios, if claims to purchase tokens in the future are granted in the course of such processes. Such uncertified securities will also be treated as securities provided they are standardised and suitable for mass trading.
- Stable coins, according to the FINMA Supplement, may classify as securities; for example, stable coins linked to commodities (other than to so-called precious metals of banks) which give rise to a contractual claim of the holder in relation to such commodities.²⁸ Also, in the case of a linkage of a stable coin to a single security by means of a token holder’s contractual delivery claim for such security, a qualification as a security may be possible according to FINMA.²⁹ Generally, if and to the extent that stable coins are designed as tokens, whose values are derived from one or more underlying asset(s) and that they provide each holder with a contractual claim to the underlying(s), irrespective of whether a physical or cash settlement is provided for (*i.e.*, redemption claim), such tokens may represent derivatives within the meaning of FinSA and FMIA (defined below). Since, under Swiss law, securities may qualify as derivatives, such stable coins may be treated as securities, in particular in the form of uncertified securities, provided that they are: (i) standardised; and (ii) suitable for mass trading.³⁰ Moreover, it cannot be excluded that certain types of stable coins may be qualified as asset tokens by FINMA since, according to FINMA, tokens that enable physical assets to be traded on a blockchain infrastructure also fall into this category (see above, “Introduction”). This might, for example, be the case for stable

coins, which merely fulfil the function of evidencing legal ownership with regard to the respective underlying such as a commodity. However, it must be noted that, from an economical perspective, where asset tokens are linked to underlyings for the main purpose of investment and therefore “represent” the respective underlyings, stable coins use such linkage primarily for the purpose of stabilisation of their price. Hence, where for asset tokens, underlyings with expected value fluctuations are of interest for investors and issuers, for stable coins, underlyings that are considered stable are of interest, in order to limit the volatility of the token’s price. The stabilisation quality of the underlyings is paramount, rather than the investment purpose or representation. This is also why relatively stable underlyings such as the U.S. Dollar or gold are often chosen. Finally, provided that, from an economical perspective, certain types of stable coins are designed in a way that they both reflect a payment as well as an investment function purpose, FINMA may qualify such coins as *hybrid tokens*.

Securities firm licence

Sales activities relating to tokens that qualify as securities may in particular trigger: (i) Swiss securities firm licence requirements under the Financial Institutions Act (“**FinIA**”);³¹ (ii) Swiss trading platform regulations under the Financial Markets Infrastructure Act (“**FMIA**”);³² and/or (iii) Swiss prospectus requirements and further regulations in connection with financial services under FinSA.

- Persons creating certain types of securities tokens and/or trading in securities tokens on behalf of his/her clients in a professional capacity may qualify as a securities firm under Swiss law and will therefore require a securities firm licence. Moreover, such trading activities may trigger various regulations under FinSA provided that, among other things, the securities firm is qualified as a “financial service provider” and the securities tokens qualify as “financial instruments” within the meaning of FinSA. For example, issuing asset tokens in the form of securities, which are linked to the performance of a share or a project, may, under certain circumstances, qualify as regulated securities firm activity. Such an issuing may also trigger the prospectus requirements under FinSA. The aforementioned licensing requirements under FinIA, however, do not apply as long as the person engaging in such activities has no physical presence (*i.e.*, no personnel and no branch) in Switzerland. Acting on a mere cross-border basis does not trigger any duty to obtain a securities firm licence. However, the regulations under FinSA, in particular, apply to persons who, in a professional capacity, provide financial services in Switzerland or to clients in Switzerland.
- Operating a platform in Switzerland that enables trading of tokens may trigger licensing requirements under the FMIA. For example, so-called “organised trading facilities” may only be operated by licensed banks, licensed securities firms or recognised (foreign) trading venues. Organised trading facilities are establishments for: (i) multilateral trading in securities or other financial instruments whose purpose is the exchange of bids and the conclusion of contracts based on discretionary rules; (ii) multilateral trading in financial instruments other than securities whose purpose is the exchange of bids and the conclusion of contracts based on non-discretionary rules; and (iii) bilateral trading in securities or other financial instruments whose purpose is the exchange of bids. Even if the types of tokens traded are limited to such that do not qualify as securities under Swiss law, a platform may still be regulated as an “organised trading facility” if the tokens traded are qualified as “other financial instruments”. Unlike for “securities”, FINMA to date has not yet offered any public guidance on whether they consider cryptocurrencies to be such “other financial instruments”.

As mentioned, the FinSA provides for a definition of the term “financial instrument” (see above, “Sales regulation”), which is commonly held to also be relevant for “organised trading facilities”. This definition of “financial instrument” is wider than the definition of securities. However, in our view, the wording of the legal definition suggests that cryptocurrencies do not qualify as financial instruments within the meaning of FinSA. This view seems to be shared by the Swiss Federal Council.³³ Should this view be followed, a platform allowing for the trading of cryptocurrencies such as Bitcoin or Ether would not be considered an “organised trading facility” and would therefore fall outside the scope of the Swiss financial regulations.

The fact that, within the current regulatory framework, organised trading facilities can only be operated by licensed banks, licensed securities firms or recognised (foreign) trading venues has been viewed by the Federal Council as problematic because companies cannot obtain any of these licences if they do not actually (also) carry out the activities of a bank, a securities firm or a recognised (foreign) trading venue (in this case, according to current FINMA practice, they are not eligible for any such licence).³⁴ In order to mitigate this issue, the legal term “securities firm” under the DLT-Draft Law will be expanded and will also apply to any person who conducts proprietary trading, is mainly active on the financial markets and operates organised trading facilities pursuant to art. 42 FMIA. This is expected to open up new business opportunities for certain market participants and allow them to exercise their business model within the framework of a regulated and supervised activity.³⁵

- The DLT-Draft Law also provides for the introduction of a new licensing category as a DLT-Trading Venue under the FMIA. Licensed DLT-Trading Venues will be authorised to provide services in the areas of trading, clearing, settlement and custody of DLT-Securities to both regulated and unregulated financial market participants, potentially including retail investors. Under certain conditions, the trading of cryptocurrencies may also be permitted at a DLT-Trading Venue.³⁶ The licensing requirements for DLT-Trading Venues are mainly based on the existing requirements for trading venues (such as stock exchanges and multilateral trading facilities). However, the FMIA will provide for specific rules for DLT-Trading Venues governing, namely, the admission of participants and the respective DLT-Securities. Moreover, the DLT-Draft Law also provides for the possibility that DLT-Trading Venues are allowed to operate organised trading facilities.

Taxation

Cryptocurrencies held by individuals

Wealth tax

For the purpose of tax assessment, cryptocurrencies must be converted into Swiss francs.³⁷ The Federal Tax Administration (“FTA”) provides year-end conversion rates for certain cryptocurrencies such as Bitcoin, Ethereum, Ripple, Bitcoin Cash and Litecoin. According to the understanding of different cantonal tax authorities, cryptocurrencies are considered to be assets, comparable with bank deposits, and are therefore subject to wealth taxes. If the FTA does not determine a year-end market value, the cryptocurrencies must be declared at the year-end price of the trading platform via which the buying and selling transactions are executed. If no current valuation rate can be determined, the cryptocurrency must be declared at the original purchase price in Swiss francs (cost of acquisition). Because the rules for declaring the cryptocurrencies can vary, the rules must first be checked in the canton of residence.

Income tax

In general, capital gains on assets of individuals such as cryptocurrencies are exempt from income tax.

However, if cryptocurrencies are held as part of the business assets of an individual (*e.g.*, because the individual is classified as a professional securities firm based on the principles laid out in circular no. 36 of the FTA), capital gains of cryptocurrencies are subject to income tax.

Cryptocurrencies held by legal entities

Capital tax

Legal entities are subject to annual capital tax. Therefore, legal entities have to declare cryptocurrencies in their tax assessment at cost of acquisition or, if this value is lower, converted at the year-end exchange rate provided by the FTA. Therefore, cryptocurrencies with no market value provided by the FTA are to be declared at acquisition costs.

Corporate income tax

Corporations are subject to Swiss corporate income tax on any net taxable earnings from the sale of cryptocurrencies. Non-realised gains on cryptocurrencies are only subject to Swiss corporate income tax in case of a mark-to-market accounting in the Swiss generally accepted accounting principles (“GAAP”) accounts of the corporate investor.

Value-added tax

For the purpose of value-added tax (“VAT”), cryptocurrencies are treated the same way as legal tender, meaning that the trading or exchange activities of cryptocurrencies and additional services related to such trading or exchange activities are exempt from VAT.³⁸

Money transmission laws and anti-money laundering requirements

Under Swiss law, both issuing cryptocurrencies as well as the subsequent trading of such tokens may be subject to anti-money laundering requirements.

The relevant starting point is to ask whether a person/company engages in any activities that constitute so-called “financial intermediation” and is hence considered a financial intermediary under the Swiss Anti-Money Laundering Act (“AMLA”).³⁹

There are two main groups of financial intermediaries. First, regulated financial intermediaries belonging to the “banking sector”, and second, other financial intermediaries belonging to the “non-banking sector”:

- Financial intermediaries belonging to the “banking sector” are companies that are subject to comprehensive, prudential regulation under special legislation, covering the whole range of their activities. Such financial intermediaries are, for example, banks or securities firms.
- Financial intermediaries belonging to the “non-banking sector” are any persons/companies that, on a professional basis: (i) accept or hold deposit assets belonging to third parties; (ii) assist in the investment of such assets; or (iii) assist in the transfer of such assets. This general definition covers, for example, persons/companies that provide services related to payment transactions, hold securities as deposits or manage securities. Whether such activity is carried out in a professional capacity or not must be assessed based on quantitative benchmarks (*e.g.*, gross margin of CHF 50,000 *p.a.*, business relationships with more than 20 parties *p.a.*, unlimited control over third-party assets exceeding CHF 5m at any time, or transaction volume exceeding CHF 2m per calendar

year). Prior to engaging in financial intermediation, such persons/companies must either join a Swiss self-regulatory organisation (“SRO”) or request a licence from FINMA in order to become a so-called directly supervised financial intermediary (“DSFI”).

The AMLA and implementing regulations provide for a series of obligations that financial intermediaries must adhere to, *e.g.*, regarding the verification of the identity of customers/contracting parties as well as the beneficial owners of funds held.

With regard to cryptocurrencies, the following is important concerning anti-money laundering regulations:

- *Primary market/ICOs*: According to FINMA, issuing cryptocurrencies (*e.g.*, payment tokens and/or stable coins) constitutes financial intermediation (issuance of a means of payment).⁴⁰
- *Secondary market/sales and trading*: Merely selling cryptocurrencies to another party, or using such cryptocurrencies as means of payment for the sale or purchase of goods and services, does not constitute financial intermediation. However, specific rules would apply if cryptocurrencies (*e.g.*, stable coins) are qualified as securities and/or as derivatives linked, in particular, to securities, commodities, precious metals, currencies or money market instruments (see above, “Sales regulation”). Also, depending on the services offered by the relevant person/company, activities relating to sales and trading may constitute financial intermediation, whenever a person/company on a professional basis: (i) accepts or holds cryptocurrencies belonging to third parties as a deposit; (ii) assists in the investment of cryptocurrencies; or (iii) assists in the transfer of cryptocurrencies.

Promotion and testing

Switzerland has not established any “sandbox” exemptions or similar arrangements that specifically focus on DLT or cryptocurrencies.

However, there are specific rules in place, which aim at generally promoting FinTech developments in Switzerland.

In 2016, the Swiss government announced that it plans on reducing barriers to market entry for FinTech businesses.⁴¹ This legislative initiative has been implemented and consists of three pillars.

- The first pillar, in force since August 1, 2017, the Swiss “sandbox” exemption, allows companies to engage in activities that would usually trigger bank licensing requirements. According to the Swiss Banking Act (“BA”),⁴² only licensed banks are allowed to accept deposits from the public in a professional capacity. Any person or entity continuously accepting more than 20 deposits from the public or publicly advertising to accept deposits is deemed to be acting in a professional capacity.⁴³ Under the sandbox exemption, companies accepting deposits are not considered to be acting in a professional capacity if: (i) the deposits accepted do not exceed the threshold of CHF 1m; (ii) the deposits accepted are neither invested nor interest-bearing; and (iii) the investors are informed in advance, in writing or in another form that provides for a record in text form, that the company is not supervised by FINMA and that the deposits are not protected by the Swiss deposit insurance regime. If the threshold of CHF 1m is exceeded, the company must notify FINMA within 10 days and file for a banking licence.
- The second pillar, in force since August 1, 2017, provides that funds held in customer accounts of asset managers, securities firms, dealers of precious metals or similar companies, which exclusively serve the purpose of settling customer transactions, do not qualify as deposits and therefore do not trigger bank licensing requirements,

provided the funds are not interest-bearing and provided that they are forwarded within up to 60 days. However, FINMA clarified that this “settlement accounts exemption” will not apply to cryptocurrency traders that execute a similar activity as foreign exchange traders by maintaining accounts for their clients for investments in different currencies. Under what circumstances a particular activity is considered to be similar to the activities of foreign exchange traders is currently not clear.

- The third pillar, in force since January 1, 2019, provides for a so-called “simplified” FinTech licence, which allows the respective licence holder to accept deposits up to the threshold of CHF 100m, provided that the deposits are neither invested nor interest-bearing. The FinTech licence, however, does not allow the offering and provisions of loans and mortgages. Therefore, it will be predominately crowdfunding platforms that will benefit from the simplified licence. The implementing Ordinance provides for a number of simplified requirements, relating to the required minimum capital, organisation and risk management, which must be satisfied in order to obtain a FinTech licence.

Ownership and licensing requirements

Ownership

Whether tokens can actually be “owned” within the meaning of Swiss ownership laws depends, in particular, on the question of whether they qualify as securities or not. Under Swiss law, it is undisputed that securities may be legally owned. With regard to tokens that do not qualify as securities, *i.e.*, cryptocurrencies such as Bitcoin, the ownership question is currently unresolved. The majority of Swiss scholars are currently of the view that, due to their lack of tangibility and for other reasons, cryptocurrencies are not a “thing” (*Sache*) in the sense of Swiss civil law.⁴⁴

Licensing requirements

There are no licences/authorisations specifically relating to cryptocurrencies (*e.g.*, stable coins) in Switzerland and, therefore, a variety of regulatory licences may be relevant in the area of cryptocurrencies, in particular (but not limited to) the banking licence and the securities firm licence (see above, “Sales regulation”).

Under Swiss law, only banks are allowed to accept deposits from the public on a professional basis (see above, “Promotion and testing”). Regulated deposit-taking may become an issue for service providers offering to store customers’ cryptocurrencies, in particular. It is currently not clear under which circumstances such service providers qualify as banks. This depends, in particular, on how the cryptocurrencies are being stored and the technical details of how such storage occurs. FINMA’s current position is that no banking licence is required if (i) cryptocurrencies “are transferred for safekeeping only”, (ii) these transferred cryptocurrencies are “stored separately on the blockchain for each customer”, and (iii) “each deposit can be attributed to an individual customer at all times”.⁴⁵ However, the DLT-Draft Law provides for an addition to the “FinTech” provision in the BA (see above, “Promotion and testing”). This addition requires any person mainly active in the financial markets, who in a professional manner accepts and stores certain crypto-based assets designated by the Federal Council or publicly recommends itself for such service, to obtain a FinTech licence (see above, “Promotion and testing”), whereby such crypto-based assets may not be invested nor interest-bearing.⁴⁶ Because of their comparability with fiat money, it is expected that the Federal Council will designate payment tokens which are stored collectively, such as crypto-based assets.⁴⁷ This adjustment takes account of the fact that under the DLT-Draft Law, crypto-based assets held in collective custody

may also be segregated in insolvency proceedings under certain circumstances (see below, “Insolvency”) and therefore such asset, according to the Dispatch, would not qualify as a deposit from the public, the acceptance of which under certain circumstances requires a banking licence under the existing regulations (see above, “Promotion and testing”).⁴⁸ Moreover, for crypto-based assets that banks hold as deposit assets for custodian clients, FINMA may, under the DLT-Draft Law, set a maximum amount on a case-by-case basis if this appears necessary due to the risks associated with such business.⁴⁹

Specifically, with regard to stable coins, no general statement is possible whether financial market activities in connection with such coins require any financial market licence. The supervisory classification of stable coins by FINMA follows the following three principles: “substance over form”; “same risks, same rules”; and “case-by-case analysis taking into account the specific circumstances of the individual case”.⁵⁰ No specific regulations for stable coins exist in Switzerland. Depending on their design features, stable coins must therefore be analysed on a case-by-case basis to determine whether any such licence is required. Design features such as (i) whether a single underlying or a basket of underlyings is used, (ii) the type of underlying, as well as (iii) if the stable coin in question gives the holder a contractual redemption claim with regard to the underlying(s), respectively, the value of the underlying(s), or if the token merely fulfils the function of evidencing an ownership position with regard to the underlying(s), may be decisive.⁵¹ In particular, a banking licence may be required. For example, according to the FINMA Supplement, in particular issuers of stable coins that are linked to (i) fiat currency applying a fixed ratio (*e.g.*, 1 token = 1 USD), or (ii) so-called precious metal of banks that provide for a contractual claim for the respective underlying, may require a banking licence.⁵² Moreover, among others, for a securities firm, a payment system licence or a licence in connection with collective investment schemes could be required. For instance, FINMA may qualify a currency, security or commodity-linked stable coin that provides each holder with a redemption claim, whose value is derived from the value of a basket containing various currencies, securities, and commodities, as a collective investment scheme, provided that the underlying assets contained in such basket are managed by the issuer for the account and risk of the token holders. The latter, according to FINMA, mainly means that all opportunities and risks of asset management in the form of profits or losses due to, among other things, interest rates, fluctuations in the value of the underlying assets, and counterparty and operational risks, are borne by the holders of the stable coin in question.⁵³ Likewise, stable coins that are linked to individual properties or a portfolio of properties may, according to FINMA, represent collective investment schemes.⁵⁴

With regard to licensing requirements, it must further be kept in mind that Switzerland implemented the new FinIA along with the FinSA in 2020. These new acts set forth a new licensing requirement for individual asset managers and a registration requirement for client advisors. Such registration will be subject to certain requirements such as proof of sufficient education, training and professional experience in the respective area of practice.

Insolvency

Under the current Swiss insolvency regime, it is not sufficiently clear whether cryptocurrencies could be segregated in favour of the entitled creditors if a third-party custodian, such as a wallet provider, were to enter into bankruptcy proceedings. In view of these uncertainties, the DLT-Draft Law suggests certain amendments to the Swiss Debt Enforcement and Bankruptcy Act, in order to allow the segregation of cryptocurrencies for the bankruptcy estate of an insolvent third-party custodian.

The segregation in favour of the creditor will, however, among other things, require that the cryptocurrencies or tokens in question can unambiguously be allocated to the respective creditor, whereby this allocation can be achieved via the distributed ledger itself or by other means, such as an internal register reflecting the respective cryptocurrency accounts of the respective creditors outside the distributed ledger or by giving each token a specific serial number that can be allocated to the respective creditors.⁵⁵ Alternatively, the DLT-Draft Law also permits a segregation if the cryptocurrencies or tokens cannot be individually assigned to the entitled person, but belong to a collective and are held in collective custody. However, in such a case, the proportion of the collective's tokens, respective of the tokens held in collective custody to which each and every entitled person is entitled, must be apparent. In this case, the proportion of the (remaining) tokens to which the entitled person in question is entitled can be segregated. In this way, it is possible to keep the tokens of several customers in one collective account (or in several collective accounts).⁵⁶ Such a segregation mechanism shall also be reflected in the amended BA. Therefore, the custody set-up under which the cryptocurrencies are stored is decisive for the question whether the cryptocurrencies can be segregated in insolvency.

Mining

Switzerland has no laws or regulations that are tailor-made to the phenomenon of cryptocurrencies or mining of cryptocurrencies. Hence, mining of cryptocurrencies is permitted and the activity is not subject to particular laws and regulations.

Since the mere use of cryptocurrencies is not considered financial intermediation (see above, "Money transmission laws and anti-money laundering requirements"), mining of cryptocurrencies does not constitute financial intermediation, as far as it is for personal use.⁵⁷ Further, mining of cryptocurrencies does generally not qualify as a financial service within the meaning of FinSA.⁵⁸

Border restrictions and declaration

In Switzerland, there are no particular border restrictions or declaration requirements that would apply to cryptocurrencies.

Reporting requirements

In Switzerland, making payments with cryptocurrencies is not a regulated activity and there are no reporting requirements to be met when such payments are made.

Estate planning and testamentary succession

In Switzerland, there are no particular estate planning or testamentary succession aspects concerning cryptocurrencies.

Under Swiss law, heirs acquire the inheritance as a whole upon death of the testator by operation of law. Therefore, all possessions with an inheritable value are transferred to the heirs by universal succession.

Cryptocurrencies such as Bitcoin are considered to have an inheritable value.⁵⁹ They are part of the inheritance and are therefore transferable. Bitcoins that are recorded on a blockchain are attached to the latter. It is recommended to determine the heir of the cryptocurrency assets, thereby taking into account the value of these assets for calculating the recipient's share. Problems arise when the heir does not possess the necessary means (usually the private keys) to dispose of the inherited cryptocurrencies.

Endnotes

1. Federal Council Report – Legal framework for distributed ledger technology and blockchain in Switzerland, dated December 14, 2018 (<https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf>).
2. Cf. <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-74420.html>.
3. Cf. <https://www.admin.ch/opc/de/federal-gazette/2020/329.pdf>.
4. Cf. <https://www.newsd.admin.ch/newsd/message/attachments/35355.pdf>.
5. Cf. <https://www.finma.ch/en/news/2015/06/mm-gwv-finma-20150623/>.
6. Cf. art. 4 paragraph 2 of the Swiss Anti-Money Laundering Ordinance: “Money or asset transfer transactions are deemed to be the transfer of assets through the acceptance of cash, precious metals, virtual currencies (...).”
7. Cf. FINMA ICO Guidelines, p. 2 *et seq.* <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>.
8. Cf. for example, p. 262 *et seq.*, p. 276 *et seq.* and p. 309 of the Dispatch.
9. Federal Council Explanatory Report – DLT-Draft Law, p. 8 <https://www.newsd.admin.ch/newsd/message/attachments/56192.pdf>; ZOGG, Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung, in: recht 2019, p. 95 *et seq.* and p. 242 *et seq.* of the Dispatch.
10. Cf. <https://www.finma.ch/de/news/2019/09/20190911-mm-stable-coins/>.
11. Cf. FINMA Supplement, p. 1; HOUDROUGE/TENOT, Le droit suisse à l’heure de la technologie des registres électroniques distribués, in: Not@lex 2020, pp. 49–63, and p. 52.
12. Cf. <https://stablecoinindex.com/>.
13. Cf. <https://blockchain.capital/the-business-of-stablecoins/>; <https://blockchainwelt.de/stablecoins-sind-preisstabile-kryptowaehrungen-moeglich/>.
14. The Swiss Federal Act on Currency and Payment Instruments determines Switzerland’s legal tender. To date, only (i) coins issued by the federal government, (ii) banknotes issued by the Swiss National Bank, and (iii) Swiss franc sight deposits at the Swiss National Bank qualify as legal tender. Legal tender is considered “money” in the narrow sense and therefore an official means of payment.
15. Cf. HAUSER-SPUEHLER/MEISSER, Eigenschaften der Kryptowährung Bitcoin, in: *digma* 2018, p. 7; MÜLLER/REUTLINGER/KAISER, Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und in der Europäischen Union, in *EuZ* 2018, p. 80.
16. Federal Council Explanatory Report – DLT-Draft Law, p. 52.
17. Cf. https://www.snb.ch/en/mmr/speeches/id/ref_20180405_amr.
18. Cf. https://www.snb.ch/de/mmr/reference/pre_20191008/source/pre_20191008.de.pdf.
19. Cf. <https://www.bitcoinsuisse.com/news/canton-zug-accept-cryptocurrencies-for-tax-payment-in-2021>; <https://www.zg.ch/behoerden/finanzdirektion/direktionssekretariat/aktuell/kanton-zug-akzeptiert-ab-2021-kryptowaehrungen-fuer-steuerzahlungen>.
20. Cf. KRAMER/OSER/MEIER, Tokenisierung von Finanzinstrumenten de lege ferenda, in: *Jusletter* May 6, 2019, N 22; Dispatch, p. 107 *et seq.*
21. Cf. Message, p. 277.
22. Cf. Federal Council Explanatory Report – DLT-Draft Law, p. 29; Dispatch, p. 277.
23. According to the DLT-Draft Law, DLT-Rights may also classify as securities; cf. Dispatch, p. 309.
24. Cf. Dispatch, p. 309.
25. It must be noted that this is a novel and rapidly developing field of law and different views can be taken as to the classification of crypto assets as securities under Swiss law. In light of this, it cannot be excluded that FINMA will come to a different conclusion in

the future, in particular with regard to cryptocurrencies. FINMA noted that they would reconsider their conclusion in light of the views taken in any future case law or any new legislation in this area.

26. *Cf.* FINMA ICO Guidelines, p. 4 *et seq.*
27. Federal Act on Financial Services of June 15, 2018, SR 950.1.
28. FINMA Supplement, p. 3.
29. FINMA Supplement, p. 4.
30. *Cf.* also HOUDROUGE/TENOT, *Le droit suisse à l'heure de la technologie des registres électroniques distribués*, *Not@lex* 2020, pp. 49–63 and p. 53.
31. Federal Act on Financial Institutions of June 15, 2018, SR 954.1.
32. Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading of June 19, 2015, SR 958.1.
33. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 122; Dispatch p. 309 *et seq.*
34. *Cf.* Dispatch, p. 305; Federal Council Report – Legal framework for distributed ledger technology and blockchain in Switzerland, p. 107 *et seq.*
35. *Cf.* Dispatch, p. 305.
36. *Cf.* Federal Council Explanatory Report – DLT-Draft Law, p. 50; Dispatch, p. 311.
37. *Cf.* Swiss Legal Tech Association (SLTA), Regulatory Task Force Report, p. 33; the Federal Tax Administration publishes every year-end an exchange list (official exchange rate) for Bitcoin, Ethereum, Ripple, Bitcoin Cash, Litecoin, Cardano, NEM, Stellar, IOTA and Tron.
38. *Cf.* Swiss Legal Tech Association (SLTA), Regulatory Task Force Report, p. 33.
39. Federal Act on Anti-Money Laundering of October 10, 1997, SR 955.0.
40. *Cf.* FINMA ICO Guidelines, p. 6; FINMA Supplement, pp. 2 and 7.
41. *Cf.* <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-64356.html>.
42. Federal Act on Banks of November 8, 1934, SR 952.0.
43. *Cf.* arts 2 and 6 of the Swiss Banking Ordinance of April 30, 2014, SR 952.02.
44. *Cf.* MUELLER/REUTLINGER/KAISER, p. 86 *et seq.*; MAURENBRECHER/MEIER, *Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen*; EGGEN, *Chain of Contracts – Eine privatrechtliche Auseinandersetzung mit Distributed Ledgers*, *AJP* 2017, p. 14; BÄRTSCHI/MEISSER, *Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht*, in: WEBER/THOUVENIN (Hrsg.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, Zurich 2015, p. 141.
45. *Cf.* FINMA fact sheet on “virtual currencies” dated January 1, 2020, p. 2.
46. *Cf.* Dispatch, p. 301; art. 1b DLT-Draft Law (BA).
47. *Cf.* Dispatch, p. 302.
48. *Cf.* Dispatch, pp. 268 and 301; BERTSCHINGER, *Das Finanzmarktaufsichtsrecht vom vierten Quartal 2018 bis ins vierte Quartal 2019*, *SZW* 2019, pp. 676–696.
49. *Cf.* Dispatch, p. 302 *et seq.*; art. 4 *sexies* DLT-Draft Law (BA).
50. *Cf.* FINMA Supplement, p. 2.
51. *Cf.* FINMA Supplement, p. 2 *et seq.*
52. *Cf.* FINMA Supplement, p. 2 *et seq.*
53. *Cf.* FINMA Supplement, pp. 2–4.
54. *Cf.* FINMA Supplement, p. 4.
55. *Cf.* Dispatch, p. 293 *et seq.*; art. 242a DLT-Draft Law (Federal Act on Debt Enforcement and Bankruptcy, of April 11, 1889, SR 281.1).

-
56. *Cf.* Dispatch, p. 239 *et seq.*; art. 242a DLT-Draft Law (Federal Act on Debt Enforcement and Bankruptcy, of April 11, 1889, SR 281.1).
 57. See also, Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 139.
 58. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 117.
 59. *Cf.* EIGENMANN/FANTI, Successions, Données Personnelles, Numériques et Renseignements, in: SJ 2017 II, p. 198.

* * *

Acknowledgment

The authors acknowledge with thanks the contributions of Marc Abplanalp to this chapter.

**Daniel Haerberli****Tel: +41 43 222 16 33 / Email: daniel.haerberli@homburger.ch**

Daniel Haerberli is a banking and finance as well as a capital markets transactions and financial market regulations specialist. He is particularly focused on secured lending, syndicated debt and structured financing as well as derivatives, securitised structured products, investment funds and bond offerings. He regularly advises clients on initial coin offerings (ICOs) and on cryptocurrency matters.

Daniel Haerberli heads the “Legal & Regulation” working group of the Swiss Structured Products Association (SSPA).

**Stefan Oesterhelt****Tel: +41 43 222 12 65 / Email: stefan.oesterhelt@homburger.ch**

Stefan Oesterhelt’s practice focuses on tax law, in particular international tax law, mergers and acquisitions, capital market transactions and tax litigation. He is a lecturer on tax law at the University of Sankt Gallen and regularly speaks at seminars on tax law.

**Alexander Wherlock****Tel: +41 43 222 17 50 / Email: alexander.wherlock@homburger.ch**

Alexander Wherlock’s practice focuses on financial markets and banking law, financial services regulation as well as corporate and commercial law. Alexander Wherlock is also a member of Homburger’s “Technology and Digital Economy” practice group.

Homburger AG

Hardstrasse 201, 8005 Zurich, Switzerland
Tel: +41 43 222 10 00 / URL: www.homburger.ch

Taiwan

Robin Chang & Eddie Hsiung
Lee and Li, Attorneys-at-Law

Government attitude and definition

Cryptocurrencies, which are not linked or tied to the currency of any nation, are currently not accepted by the Central Bank of the Republic of China (Taiwan) (“CBC”) as currencies. On 30 December 2013, both the CBC and Taiwan’s Financial Supervisory Commission (“FSC”) first expressed the government’s position toward Bitcoin by issuing a joint press release (“2013 Release”). According to the 2013 Release, the two authorities held that Bitcoin should not be considered a “currency”, but a highly speculative digital “virtual commodity”. In another FSC press release in 2014 (“2014 Release”), the FSC ordered that local banks must not accept Bitcoin or provide any other services related to Bitcoin (such as the exchange of Bitcoins for fiat currency). The FSC further issued a press release on 19 December 2017 (“2017 Release”), in which the FSC reiterated the government’s position as specified in the 2013 and 2014 Releases.

Other than the above, no laws, regulations or rulings have been officially issued, promulgated or amended to specifically deal with the rise of cryptocurrencies, except for the regulations governing offering and issuance of any tokens with the nature of securities (which are commonly called “security tokens”, and their offering commonly called “security token offerings” (“STOs”)) as discussed under “Sales regulation” below.

Cryptocurrency regulation

Please see “Government attitude and definition” above. So far, except for the STO regulations discussed under “Sales regulation” below, no Taiwanese laws or regulations have been promulgated or amended to formally regulate “virtual currencies” or “cryptocurrencies”; therefore, virtual currencies/cryptocurrencies cannot currently be considered “legal tender”, “currencies” or a generally accepted “medium of exchange” in Taiwan.

Further, there currently exists no required licence in Taiwan for (a) operating the services of exchange between virtual currencies or virtual currencies with fiat currencies, or (b) acting as a “money transmitter” and the like in Taiwan.

Sales regulation

Sale of Bitcoins or any other virtual currencies/cryptocurrencies of the same nature and characteristics

So far, except for the STO regulations discussed below, there exist no laws or regulations specifically dealing with the sale of virtual currencies/cryptocurrencies. The sale of Bitcoins, currently considered by the FSC a sale of a digital “virtual commodity” but not “currency”, should generally be fine from a Taiwan regulatory perspective, and the general

principles and rules governing “purchase and sale” under the Civil Code would apply if the consideration is cash. Also, we tend to think that the above would apply to the sale of other virtual currencies/cryptocurrencies of the same nature and characteristics as Bitcoin.

Please note that the above is subject to “ICO and token offering” as described below.

ICO and token offering

In response to the rising amount of initial coin offerings (“ICOs”) and other investment activities regarding virtual currencies/cryptocurrencies, the FSC also expressed the following view on ICOs through the 2017 Release as mentioned above:

- (1) An ICO refers to the issue and sale of “virtual commodities” (such as digital interests, digital assets, or digital virtual currencies) to investors. The classification of an ICO should be determined on a case-by-case basis. For example, if an ICO involves the offer and issue of “securities”, it should be subject to Taiwan’s Securities and Exchange Act (“SEA”). The issue of whether tokens in an ICO would be deemed “securities” under the SEA would depend on the facts of each individual case.
- (2) If any misrepresentations with respect to technologies or their outcomes, and/or promises of unreasonably high returns are used by the issuer of virtual currencies or an ICO to attract investors, the issuer would be deemed to be committing fraud or illegal fundraising.

Given the above, in an ICO (or other type of token offering, such as private token pre-sale before the ICO stage), the core issue in this regard is whether an ICO would be considered an issuing of “securities” under Taiwan’s securities regulations. Under current Taiwan law, the offer and sale of “securities” in Taiwan, whether through public offering or private placement, are regulated activities and shall be governed in accordance with the SEA and its related regulations as well as relevant rulings issued from time to time by the FSC.

Security tokens and STOs

On 3 July 2019, the FSC, by issuing a ruling, officially designated cryptocurrencies with the nature of securities, i.e. security tokens, as “securities” under the SEA (the “2019 Ruling”). According to the 2019 Ruling, security tokens refer to those that:

- utilise cryptography, distributed ledger technology or other similar technologies to represent their value that can be stored, exchanged or transferred through a digital mechanism;
- are transferable; and
- encompass all of the following attributes of an investment:
 - funding provided by investors;
 - providing funding for a common enterprise or project;
 - investors expecting to receive profits; and
 - profits generated primarily from the efforts of the issuer or third parties.

In addition to the 2019 Ruling, the FSC issued a press release on 27 June 2019 to illustrate the key points of FSC’s policy on STOs. Since then, the FSC and the Taipei Exchange (“TPEX”) have been setting out the set of regulations governing STOs, and the STO regulations were finalised in January of 2020. Specifically, the FSC differentiates the regulation of STOs with the threshold of 30 million New Taiwan Dollars (NT\$). For an STO of NT\$30 million or less, the STO may be conducted in compliance with the STO regulations; an STO above NT\$30 million must first apply to be tested in the “financial regulatory sandbox” pursuant to the Sandbox Act and, in case the experiment has a positive outcome, should be conducted pursuant to the SEA. Please see the below summary of certain key provisions of the STO regulations (i.e. for STOs of NT\$30 million or less).

Qualifications of the issuer – the issuer must be a company limited by shares incorporated under the laws of Taiwan and not a company listed on the Taiwan Stock Exchange or TPEX or traded on the Emerging Stock Market.

Types of security tokens that can be issued – the issuer can only issue profit-sharing or debt tokens without shareholders' rights.

Eligible investors and amount limits – only “professional investors” are eligible to participate in STOs; where the professional investor is a natural person, the maximum subscription amount is NT\$300,000 per STO.

STO platform operator

- Qualifications of the platform operator – the platform operator should obtain a securities dealer licence, have a minimum paid-in capital of NT\$100 million and provide an operation bond in the amount of NT\$10 million.
- Total offering amount capacity – the total offering amount of all STOs on a single platform should not exceed NT\$100 million. A platform can accept to process a second STO only one year after the security tokens of the first STO have been traded on the platform.
- Transfer and record-keeping – the platform operator should enter into an agreement with the Taiwan Depository and Clearing Corporation (“TDCC”) and transmit the trading information, such as balance changes and a balance statement, to the TDCC for its record on a daily basis. The TDCC should provide an STO balance inquiry service to investors.

Pursuant to the STO regulations, there are also some other requirements and restrictions including those regarding trading (secondary market), real-name basis, NT\$ only, etc.

Taxation

There is currently no regulation specifically governing the taxation of cryptocurrencies; however, by referring to the tax laws and tax rulings in connection with the taxation of cross-border e-commerce transactions and online sales of services, it is possible that the tax authorities might take the following stances:

Business tax (also known as value-added tax or “VAT”)

The trading of cryptocurrencies on a platform within Taiwan may be deemed a sale of services within Taiwan and thus be subject to Taiwan business tax as follows:

- (i) If the seller is a Taiwan business entity, the seller will be subject to 5% VAT on the revenue.
- (ii) If the seller is a Taiwanese individual, the individual should apply for tax registration and pay 5% VAT on the revenue, unless the monthly sales amount is under NT\$40,000 (approx. US\$1,300).
- (iii) If the seller is a foreign entity with a fixed place of business in Taiwan (e.g., a Taiwan branch), the Taiwan branch should pay 5% VAT on such revenue.
- (iv) If the seller is a foreign entity without a fixed place of business in Taiwan, and the purchasers of the cryptocurrencies are entirely Taiwanese entities, the seller will have no business tax issue; instead, the purchasers will become the taxpayer.
- (v) If the seller is a foreign entity without a fixed place of business in Taiwan, and the purchasers of the cryptocurrencies include Taiwanese individuals, the foreign seller should apply for tax registration and pay 5% VAT on the revenue generated from the sale of the cryptocurrencies to the Taiwanese individuals, unless the monthly sales amount to the Taiwanese individuals is under NT\$40,000 (approx. US\$1,300).

Income tax

Any income generated from the trading of cryptocurrencies on an onshore platform (“Trading Income”) may be deemed as income sourced from Taiwan and thus be subject to Taiwan income tax as follows:

- (i) If the seller is a Taiwan business entity, the seller should consolidate the Trading Income into its other taxable income for calculating its Taiwan income tax payable. (The prevailing income tax rate is generally 20% on the net taxable income.)
- (ii) If the seller is a Taiwanese individual, the individual should consolidate the Trading Income into its other taxable income for calculating its Taiwan income tax payable. (The prevailing highest progressive tax rate is 40% on the net taxable income.)
- (iii) If the seller is a foreign entity with a fixed place of business in Taiwan (e.g., a Taiwan branch), the Taiwan branch should consolidate the Trading Income into its other taxable income and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)
- (iv) If the seller is a foreign entity with a business agent in Taiwan, the business agent should, on behalf of the foreign entity, file an income tax return, report the Trading Income, and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)
- (v) If the seller is a foreign entity without a fixed place of business or business agent in Taiwan, the seller should file an income tax return (the seller may engage a tax agent to file the tax return on its behalf), report the Trading Income, and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)

Money transmission laws and anti-money laundering requirements

As advised under “Cryptocurrency regulation” above, currently there exists no required licence for (a) operating the services of exchange between virtual currencies or virtual currencies with fiat currencies, or (b) acting as a “money transmitter” and the like in Taiwan.

As for anti-money laundering, the latest amended Money Laundering Control Act of Taiwan (“Taiwan AML Act”), which took effect on 7 November 2018, has brought the cryptocurrency platform operators into the anti-money laundering regulatory regime. However, how it will be implemented and what requirements will be imposed by the FSC (which is the main regulator of the Taiwan AML Act) are not clear at this stage in terms of anti-money laundering activities of cryptocurrency exchanges and platforms.

Promotion and testing

Taiwan’s law for the fintech regulatory sandbox, the “FinTech Development and Innovation and Experiment Act” (“Sandbox Act”), was promulgated on 31 January 2018 and took effect on 30 April 2018. The Sandbox Act was enacted to enable fintech businesses to test their financial technologies.

According to the Sandbox Act, an applicant (which can be an entity or individual) needs to obtain approval from the FSC before entering the sandbox. Once the experiment begins, the experimental activities may enjoy exemptions from certain laws and regulations (such as FSC licensing requirements and certain legal liability exemptions).

After completion of the approved experiments, the FSC will analyse the results of the experiments. If the result is positive, the FSC would actively examine the existing financial laws and regulations to explore the possibility of amending them, after which the business model or activities previously tested in the sandbox could become feasible under law.

Please note, however, that the sandbox entity or individual might still be required to apply for a relevant licence or approval from the FSC in order to formally conduct the activities as previously tested in the sandbox.

At the time of the writing, seven applications have been approved by the FSC to enter into the sandbox, but none of them are related to cryptocurrencies. Nonetheless, please note that under the STO regulations as advised above, there would be an upper limit for the total amount of an STO programme, and according to relevant news reports, the FSC mentioned that any STO exceeding such upper limit may first need to be tested and experimented with in the regulatory sandbox.

Even so, it is possible that the relevant STO market players, as well as some controversial fintech business models and activities (e.g., ICOs), would wish to apply to the FSC to enter the sandbox. However, according to the Sandbox Act, any experimental activity needs to be “innovative”. Therefore, (a) whether or not the commonly seen cryptocurrency-related activities (such as ICOs and/or STOs) would enter the sandbox, and (b) if yes, whether the result of the experiment would be considered “positive”, would still depend on the FSC’s then-effective policies and final decision.

Ownership and licensing requirements

As mentioned above, except for the STO regulations advised above, Taiwan has not promulgated any laws or regulations specifically dealing with “virtual currencies” or “cryptocurrencies”. Therefore, there exist no ownership or licensing requirements under Taiwanese law, except for the STO platform operator (which should obtain a securities dealer licence) as advised under “Sales regulation” above.

Mining

So far, no Taiwanese laws or regulations have been promulgated or amended to regulate the “mining” of Bitcoin or any other types of cryptocurrency. Mining activities are generally permitted.

Border restrictions and declaration

So far, no Taiwanese laws or regulations have been specifically promulgated or amended to impose any border restrictions on, or requirements for, declaration of holdings of cryptocurrencies.

Reporting requirements

So far, no Taiwanese laws or regulations have been specifically promulgated or amended to impose any reporting requirements for cryptocurrencies.

Estate planning and testamentary succession

So far, Taiwan’s laws and regulations have not addressed this topic. Since cryptocurrencies have value, we tend to think they would be considered “property” or “assets” from the perspective of Taiwan estate and succession law, unless they are confiscated by the government due to, for example, the commission of a criminal offence violating the prohibition of “securities” offerings without prior approval from, or registration with, the FSC as required under the SEA (see our advice under “Sales regulation” above).

**Robin Chang****Tel: +886 2 2763 8000 ext. 2208 / Email: robinchang@leeandli.com**

Mr. Robin Chang is a partner at Lee and Li and the head of the firm's banking practice group. His practice focuses on banking, IPOs, capital markets, mergers and acquisitions, project financing, financial consumer protection law, personal data protection law, securitisation and antitrust law.

Mr. Chang advises major international commercial banks and investment banks on their operations in Taiwan, including providing advice on compliance and regulatory issues, setting up a banking branch or bank subsidiary in Taiwan and customer complaints. He has been involved in many M&A transactions of financial institutions. He has also been involved in government projects in e-payment regulations in Taiwan.

**Eddie Hsiung****Tel: +886 2 2763 8000 ext. 2162 / Email: eddiehsiung@leeandli.com**

Mr. Eddie Hsiung is licensed to practise law in Taiwan and New York, and is also a CPA in Washington State, U.S.A. His practice focuses on securities, M&A, banking, finance, asset and fund management, cross-border investments, general corporate and commercial, fintech, startups, etc. He regularly advises leading banks, securities firms, payment and credit cards and other financial services companies on transactional, licensing and regulatory and compliance matters, as well as internal investigations. He is familiar with legal issues regarding the application of new technologies such as fintech (e-payment, digital financial services, and regulatory sandboxes), blockchain (ICOs, cryptocurrencies, platform operators) and AI, and is often invited to participate in public hearings, seminars and panel discussions in these areas.

Lee and Li, Attorneys-at-Law

8F, No. 555, Sec. 4, Zhongxiao East Road, Taipei 11072, Taiwan, R.O.C.

Tel: +886 2 2763 8000 / URL: www.leeandli.com

United Kingdom

Stuart Davis, Sam Maxson & Andrew Moyle
Latham & Watkins LLP

Government attitude and definition

Although still actively developing, current UK policy thinking in relation to cryptocurrencies was set out by the UK Cryptoassets Taskforce in its *Final Report*¹ (the “**Taskforce Report**”), published in October 2018.

The Taskforce Report identifies cryptocurrencies as a subset of the broader category “cryptoasset”. It defines the latter as “a cryptographically secured digital representation of value or contractual rights that uses some type of [distributed ledger technology] and can be transferred, stored or traded electronically”.² Within this overarching category, the Taskforce Report identifies three sub-categories and offers the following (non-legislative) definitions:

- A. **Exchange tokens** – which are often referred to as ‘cryptocurrencies’ such as Bitcoin, Litecoin and equivalents. They utilise a [distributed ledger technology] platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.
- B. **Security tokens** – which amount to a ‘specified investment’ as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order [...]. These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or financial instruments under the EU’s Markets in Financial Instruments Directive II [...].
- C. **Utility tokens** – which can be redeemed for access to a specific product or service that is typically provided using a [distributed ledger technology] platform.”³

Although UK financial regulators have issued warnings in relation to investment in cryptoassets,⁴ they are not subject to a blanket prohibition or ban in the UK. However, as indicated by the definitions set out in the Taskforce Report, some will be subject to financial regulation (see *Cryptocurrency regulation* below). The UK anti-money laundering (“**AML**”) regime has also been extended to capture activities relating to most cryptoassets (including cryptocurrencies), regardless of whether they are otherwise subject to financial regulation (see *Money transmission laws and anti-money laundering requirements* below).

Despite publication of the Taskforce Report, UK policy towards cryptocurrencies is still developing. In particular, the authorities making up the Taskforce are continuing to conduct further substantive work in relation to cryptocurrencies. For example, the UK Financial Conduct Authority (“**FCA**”) consulted on⁵ and published⁶ regulatory guidance in relation to cryptoassets (including cryptocurrencies) (the “**FCA Guidance**”). It has also recently consulted⁷ on a proposed ban on the sale, marketing and distribution of derivatives and exchange-traded notes referencing cryptoassets (including cryptocurrencies) to all retail

consumers. The FCA had expected to implement rules relating to the retail ban in Q2 of 2020; however, owing to COVID-19, it delayed the implementation to the second half of 2020. At the time of writing, HM Treasury is also consulting on changes to the UK financial promotions regime with a view to bringing otherwise unregulated cryptoassets (including cryptocurrencies) into scope (see *Sales regulation* below).

Cryptoassets (including cryptocurrencies) are not considered money or equivalent to fiat currency in the UK. For the time being, the Bank of England has not made a decision on whether to introduce a central bank digital currency,⁸ and has launched a discussion paper on what such a central bank digital currency would look like.⁹

Cryptocurrency regulation

As noted above, there is no blanket prohibition or ban on cryptocurrencies in the UK. Nor does the UK have a bespoke financial regulatory regime for cryptoassets (notwithstanding that certain elements of the UK AML regime apply specifically in relation to cryptoasset business). Accordingly, whether or not a given cryptocurrency is subject to financial regulation in the UK depends on whether it falls within the general financial regulatory perimeter established under the Financial Services and Markets Act 2000 (“**FSMA**”) or, as discussed in *Money transmission laws and anti-money laundering requirements* below, the AML regime or under the payment services and electronic money regime established under the Payment Services Regulations 2017 (“**PSRs**”) and the Electronic Money Regulations 2011 (“**EMRs**”).

This is reflected in the cryptoasset “taxonomy” set out in the FCA Guidance which broadly follows the definitions set out in the Taskforce Report, but which has been refined by the FCA as follows:

Taskforce Report taxonomy	FCA Guidance taxonomy ¹⁰
<p>Security tokens – which amount to a ‘specified investment’ as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order [...]. These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or financial instruments under the EU’s Markets in Financial Instruments Directive II [...].</p>	<p>Security tokens: These are tokens that amount to a ‘Specified Investment’ under the Regulated Activities Order (RAO), excluding e-money. These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or other financial instrument under the EU’s Markets in Financial Instruments Directive II (MiFID II). These tokens are likely to be inside the FCA’s regulatory perimeter.</p> <p>E-money tokens: These are tokens that meet the definition of e-money under the Electronic Money Regulations (EMRs). These tokens fall within regulation.</p>
<p>Exchange tokens – which are often referred to as ‘cryptocurrencies’ such as Bitcoin, Litecoin and equivalents. They utilise a [distributed ledger technology] platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.</p>	<p>Unregulated tokens: Any tokens that are not security tokens or e-money tokens are unregulated tokens. This category includes utility tokens which can be redeemed for access to a specific product or service that is typically provided using a DLT platform.</p> <p>The category also includes tokens such as Bitcoin, Litecoin and equivalents, and often referred to as ‘cryptocurrencies’, ‘cryptocoins’ or ‘payment tokens’. These tokens are usually decentralised and designed to be used primarily as a medium of exchange. We sometimes refer to them as exchange tokens and they do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.</p>

In summary, the FCA Guidance taxonomy splits cryptoassets into regulated and unregulated cryptoassets. The Taskforce Report definitions of exchange tokens and utility tokens are retained and these two sub-categories of cryptoassets comprise “unregulated tokens” in the FCA Guidance taxonomy. Cryptoassets that constitute electronic money are split out from the Taskforce Report sub-category of security tokens, instead being labelled as “e-money tokens”, and these two sub-categories of cryptoassets (i.e., security tokens other than e-money tokens and e-money tokens) comprise “regulated tokens” in the FCA Guidance taxonomy.

The kinds of instruments that are regulated under FSMA are set out in an exhaustive fashion in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (“RAO”). These are known as “specified investments” and include instruments such as shares, bonds, fund interests and derivative contracts. Therefore, in order to determine whether a given cryptocurrency is subject to financial regulation in the UK, it is necessary to analyse whether it matches the definition of any specified investment in the RAO. Those cryptoassets that do are labelled “security tokens” in the FCA Guidance and will typically be subject to UK financial regulation.

As stated by the FCA: “Any tokens that are not security tokens or e-money tokens [as to which see *Money transmission laws and anti-money laundering requirements*] are unregulated tokens.”¹¹ In practice, this analysis proceeds predominantly on the basis of an “intrinsic” assessment of a given cryptocurrency, focused on the rights or entitlements granted to holders, rather than being based on “extrinsic” factors, such as the intended or actual use of the relevant cryptocurrency or other contextual factors relating to the cryptoasset (such as whether a platform to which the cryptoasset relates is currently operational or whether the network underlying the cryptoasset is decentralised).¹²

Although characterisation of cryptocurrencies in this way must be undertaken on a case-by-case basis in order to determine definitively whether they are subject to UK financial regulation, the FCA Guidance provides useful indicators of the likely outcome of any such analysis. “Classic” cryptocurrencies (such as Bitcoin, Litecoin and Ether) which are not centrally issued and give no rights or entitlements to holders are labelled “exchange tokens” in the Taskforce Report and “unregulated tokens” in the FCA Guidance. As explained in the FCA Guidance, exchange tokens “typically do not grant the holder any of the rights associated with specified investments”.¹³ Accordingly, in the FCA’s view:

“Exchange tokens currently fall outside the regulatory perimeter. This means that the transferring, buying and selling of these tokens, including the commercial operation of cryptoasset exchanges for exchange tokens, are activities not currently regulated by the FCA.

“For example, if you are an exchange, and all you do is facilitate transactions of Bitcoins, Ether, Litecoin or other exchange tokens between participants, you are not carrying on a regulated activity.”¹⁴

It is therefore clear that activities in relation to Bitcoin, Litecoin and Ether are currently unlikely to trigger licensing requirements in the UK (although registration under the recently extended UK AML regime may be required). Cryptocurrencies with substantially similar features (i.e., those that are not centrally issued and do not grant any rights or entitlements to holders) are also currently unlikely to trigger licensing requirements in the UK (although, again, registration under the UK AML regime may be required). The fact that they may be used for speculative investment purposes in addition to being used as a means of exchange should not impact this conclusion.

One increasingly popular type of cryptoasset which is typically more difficult to characterise for financial regulatory purposes than classic cryptocurrencies is “stablecoins”. Broadly, a stablecoin is a cryptoasset that by design seeks to maintain a stable market value through pegging the value of the stablecoin to an underlying asset (such as gold or USD). Often, stablecoins are primarily intended to be utilised as a means of exchange much like classic cryptocurrencies. Pegging the value of a stablecoin to an underlying asset can be achieved in a variety of ways, and the precise structure adopted by a given stablecoin will determine whether it is classified as a specified investment in the UK. For example, a “fully collateralised” stablecoin issued by a central issuer, which is pegged to an underlying reference asset through the issuer holding the relevant underlying reference asset, is likely to constitute a specified investment (or, indeed, electronic money) if holders of the stablecoin have rights or entitlements in relation to the underlying reference asset. It is presently possible, however, to structure a stablecoin such that it is unregulated in the UK.

However, it is important to note that even if a given cryptocurrency is not a specified investment other than electronic money (i.e., not a security token following the FCA Guidance), certain activities in relation to such cryptocurrencies can still be subject to UK financial regulation and cryptoassets that constitute electronic money (i.e., e-money tokens following the FCA Guidance) are subject to regulation.

For example, offering to enter into derivative contracts that reference unregulated cryptocurrencies as their underlying (such as cryptocurrency contracts for differences or Bitcoin futures) way of business is likely to constitute a regulated activity in the UK for which a person would require authorisation from the FCA. Indeed, such derivatives are also the subject of the proposed FCA ban on their sale, marketing and distribution to retail customers. Establishing, operating, marketing or managing a fund that offers exposure to unregulated cryptocurrencies by way of business may also be subject to UK financial regulation. Furthermore, money transmissions laws and AML legislation may also apply to activities carried out in relation to unregulated cryptocurrencies (see *Money transmission laws and anti-money laundering requirements* below).

Sales regulation

The principal sales regulation that is potentially applicable to sales of cryptocurrencies in the UK falls into three broad categories: i) UK prospectus requirements; ii) the UK restriction on financial promotions; and iii) consumer protection and online/distance selling legislation.

UK prospectus requirements

FSMA, in conjunction with the EU Prospectus Regulation, imposes requirements for an approved prospectus to have been made available to the public before: a) transferable securities are offered to the public in the UK; or b) a request is made for transferable securities to be admitted to a regulated market situated or operating in the UK.¹⁵ Unless an exemption applies (public offers made to qualified investors are, for example, exempt), a detailed prospectus containing prescribed content must be drawn up, approved by the FCA (or the appropriate EEA Member State financial regulator where the UK is not the home state of the issuer of the transferable securities) and published before the relevant offer or request is made.

However, these requirements only apply to offers or requests relating to transferable securities. Transferable securities for these purposes are anything that falls within the definition of transferable securities in the second EU Markets in Financial Instruments

Directive (“**MiFID II**”) which captures, for example, shares, bonds, and depository receipts (and instruments that give their holders similar rights or entitlements).

Therefore, in order to determine whether these requirements apply to the sale of a given cryptocurrency in the UK, it is necessary to determine whether the cryptocurrency in question is a transferable security. Referring back to the FCA Guidance, only cryptocurrencies that are security tokens (i.e., only those cryptocurrencies that amount to a specified investment under the RAO other than electronic money) may be transferable securities.¹⁶ Classic cryptocurrencies (such as Bitcoin, Litecoin and Ether) and cryptocurrencies with substantially similar features to classic cryptocurrencies are likely to be regarded as exchange tokens, rather than security tokens. Accordingly, the UK prospectus requirements should not apply to the sales of such cryptocurrencies.

UK restriction on financial promotions

FSMA contains a restriction on financial promotions which applies independently of the UK prospectus requirements. In summary, the restriction is that a person who is not appropriately authorised must not, in the course of business, communicate an invitation or inducement to engage in investment activity in a way that is capable of having an effect in the UK unless the communication is approved by an appropriately authorised person or an exemption applies. For now, section 21(2)(b) FSMA provides that unauthorised persons may communicate financial promotions if they are approved by an authorised firm. By way of a consultation paper in July 2020, HM Treasury proposed restricting such potential back-to-back arrangements by establishing a regulatory “gateway”. As of now, legislation does not provide for the FCA to assess the suitability of an authorised firm before it begins approving financial promotions. As such, the government proposes to amend FSMA so that unauthorised persons will only be able to communicate financial promotions that have been approved by a firm that has itself obtained consent from the FCA to provide such approval. Notably, however, the government does not intend this new gateway to apply to firms approving the financial promotions of an unauthorised person within the same group, or to the approval of authorised firms’ own promotions for communication by unauthorised persons.

For these purposes, the concept of engaging in investment activity is further defined by reference to “controlled activities” and “controlled investments”, which are set out in exhaustive fashion in the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (“**FPO**”). Therefore, in order to determine whether the restriction on financial promotions applies to the sale of a given cryptocurrency, it is necessary to determine whether it involves the performance of a controlled activity or a controlled investment by reference to the definitions of each that are set out in the FPO.

By way of a consultation paper in July 2020,¹⁷ HM Treasury proposed to widen the regulatory perimeter by adding otherwise unregulated cryptoassets to the list of controlled investments and increasing the list of controlled activities to include activities relating to the buying, selling, subscribing for or underwriting of qualifying cryptoassets.

Typically, sales of classic cryptocurrencies (such as Bitcoin, Litecoin and Ether) and cryptocurrencies with substantially similar features to classic cryptocurrencies should not engage the UK restriction on financial promotions, although analysis of the sale in question must be undertaken on a case-by-case basis in order to determine definitively that this is the case (and related offerings such as funds providing exposure to unregulated cryptocurrencies may well trigger the restriction). Notably, this position may change in light of the proposed changes to the FPO noted above. Furthermore, even if a particular sale of cryptocurrencies

were *prima facie* to engage the restriction, a number of potentially helpful exemptions exist, of which the most likely to be relevant are those relating to financial promotions given to investment professionals, sophisticated investors and high-net-worth individuals/companies.

General advertising, online/distance selling and consumer protection legislation

In addition to sales regulation that arises out of the UK financial regulatory framework, there is a raft of general advertising, online/distance selling and consumer protection legislation that is potentially applicable to sales of cryptocurrencies or the offering of services related to cryptocurrencies (such as exchange or wallet services) in or from the UK.

Some, like the Consumer Rights Act 2015 or the Consumer Protection from Unfair Trading Regulations 2008, only apply in relation to consumers (typically defined as individuals acting outside of their trade, business, craft or profession) but where they do, provide consumers with significant statutory rights and remedies against supplies of goods, services and digital content and impose restrictions on the kinds of contractual terms that can be enforced against consumers. Others, like the Electronic Commerce (EC Directive) Regulations 2002, are of more general application and impose requirements on businesses established in the UK that offer or provide goods or services digitally. The application of such legislation may also depend on whether or not the business being conducted is subject to UK financial regulation.

Taxation

Currently, there are no bespoke UK tax rules applicable to cryptocurrencies. Therefore, existing tax principles and rules apply generally (although some uncertainty remains as to their application).

The UK tax authority HM Revenue and Customs (“**HMRC**”) considers that cryptoassets are cryptographically secured digital representations of value or contractual rights that can be transferred, stored and traded electronically (i.e., the definition adopted by the Taskforce). In line with the Taskforce Report, HMRC has identified three types of cryptoassets – exchange tokens, utility tokens and security tokens. However, HMRC will look at the facts of each case and apply the relevant tax provisions according to what has actually taken place. The classification of cryptoassets is not necessarily determinative of their tax treatment, which will depend on the nature and use of the cryptoasset in question.

Although there is no definitive policy towards the taxation of cryptoassets (including cryptocurrency) in the UK, HMRC has published two policy papers, one relating to the taxation of cryptoassets for individuals, published in December 2018 (and updated in December 2019), and the other relating to the taxation of cryptoassets for businesses, published in December 2019 (though note that the position in these papers may not be binding on HMRC).

The policy papers focus on the taxation of exchange tokens. For security tokens and utility tokens, the guidance may provide the starting principles, but different tax treatments may need to be adopted and further HMRC guidance may be published in due course.

*Cryptoassets: tax for individuals*¹⁸ sets out HMRC’s views about how individuals who hold exchange tokens are to be taxed. This policy paper includes the following helpful general points:

- Capital Gains Tax (“**CGT**”) and Income Tax (“**IT**”) may apply to dealings in cryptocurrencies depending on the circumstances. HMRC has clarified that it does not regard cryptocurrencies as currency or money, and that it does not consider buying and

selling cryptocurrencies to be the same as gambling (which largely rules out arguments that cryptocurrencies could be exempt from taxation). Cryptoassets will be property for the purposes of Inheritance Tax.

- In most cases, HMRC expects that buying and selling of cryptocurrencies by an individual will amount to personal investment activity, meaning that individuals will typically have to pay CGT on any gains they realise upon disposal of the cryptocurrencies (which includes not only selling them for fiat currency but also using them to pay for goods and services, giving them away to another person and exchanging them for another kind of cryptoasset).
- However, if (exceptionally, in HMRC's view) an individual is engaged in a trade of dealing in cryptocurrencies (to be determined in accordance with the existing approach taken towards determining whether an individual is engaged in trading securities and other financial instruments for tax purposes), IT would take priority over CGT, being applied to the individual's trading profits.
- Individuals will be liable to pay IT and National Insurance contributions on cryptocurrencies that they receive as a form of payment from their employer. If the cryptocurrencies are considered readily convertible assets ("RCAs"), the IT liability will need to be accounted through Pay-As-You-Earn ("PAYE"), and employer National Insurance contributions will also be due. Cryptocurrencies that are not RCAs are still subject to IT and National Insurance contributions, but employers do not have to operate PAYE. The individual must declare and pay HMRC the IT due on any amount of employment income received in the form of cryptoassets. The employer should treat the payment of cryptoassets, which are not RCAs, as payments in kind for National Insurance contributions purposes, and pay any Class 1A National Insurance contributions to HMRC. Broadly, a cryptocurrency will be an RCA if trading arrangements exist, or are likely to come into existence.
- A charge to CGT may also arise if an individual subsequently disposes (other than in the course of a relevant trade) of cryptocurrencies received from their employer, as a result of mining activity or airdrops regardless of whether or not IT was payable on their receipt.
- If a person is resident but not domiciled in the UK and claims the remittance basis of taxation, income and gains that have a source outside the UK are usually only taxed if they are remitted to the UK. HMRC has taken the view that throughout the time an individual is a UK resident, the exchange tokens they hold as beneficial owner will be located in the UK. As a result, UK resident individuals (whether UK or non-UK domiciled) will be subject to UK tax if they carry out a transaction with their tokens that is subject to UK tax.

Cryptoasset exchanges may only keep records of transactions for a short period, or the exchange may no longer be in existence when an individual completes a tax return. The onus is therefore on the individual to keep separate records for each cryptoasset transaction, and these must include:

1. the type of cryptoasset;
2. the date of the transaction;
3. if the cryptoasset was bought or sold;
4. the number of units;
5. the value of the transaction in pound sterling;
6. the cumulative total of the investment units held; and
7. bank statements and wallet addresses, if needed for an enquiry or review.

*Cryptoassets: tax for businesses*¹⁹ sets out HMRC's views about how transactions involving cryptoasset exchange tokens that are undertaken by companies and other businesses (including sole traders and partnerships) are to be taxed. This policy paper includes the following helpful general points:

- As HMRC does not consider any of the current types of cryptoassets to be money or currency, any corporation tax legislation that relates solely to money or currency does not apply to exchange tokens or other types of cryptoassets (e.g., the foreign currency rules, the Disregard Regulations relating to exchange gains and losses, and designated currency elections).
- Where the buying and selling, or mining, of exchange tokens amounts to a trade, the receipts and expenses of the trade will form part of the calculation of the trading profit of that business for corporation tax purposes. For example, if a company carrying on a trade accepts exchange tokens as payment from customers, or uses them to make payments to suppliers, the token given or received will need to be accounted for within the taxable trading profits. Similarly, in respect of mining, if a business purchases a bank of dedicated computers to mine exchange tokens, as opposed to mining using excess home computer capacity, the cryptoassets mined will probably amount to trade receipts and be taxed in accordance with corporation tax principles.
- If the activity concerning the exchange token is not a trading activity, and is not charged to corporation tax in another way (such as the non-trading loan relationship or intangible fixed asset rules), then the activity may be the disposal of a capital asset. Any gain that arises from the disposal would typically be charged to corporation tax as a chargeable gain. A disposal for these purposes includes not only selling tokens for fiat currency, but also using them to pay for goods and services, giving them away to another person and exchanging them for another kind of cryptoasset.
- Companies that account for exchange tokens as “intangible assets” may be taxed under corporation tax rules for intangible fixed assets if the token is both an “intangible asset” for accounting purposes and an “intangible fixed asset”. This means it has been created or acquired by a company for use on a continuing basis. Exchange tokens that are simply held by the company, even when held in the course of its activities, will not meet this definition. If these conditions are met, the corporation tax rules for intangible fixed assets (Corporation Tax Act 2009 Part 8) have priority over the chargeable gains rules.
- A company has a “loan relationship” if it has a money debt that has arisen from a transaction for the lending of money. HMRC does not consider exchange tokens to be money. In addition, there is typically no counterparty standing behind the token and, as such, the token does not seem to constitute a debt. This means that exchange tokens do not create a loan relationship. If exchange tokens have been provided as collateral security for an ordinary loan (of money), a loan relationship exists and the loan relationship rules will apply (whether the company is the debtor or creditor).
- Value-Added Tax (“VAT”) is due in the normal way on any VAT-able goods or services sold in exchange for exchange tokens. The value of the supply of goods or services on which VAT is due will be the pound sterling value of the exchange tokens at the point the transaction takes place.
- Stamp duty and Stamp Duty Reserve Tax (“SDRT”) will not usually be chargeable on the transfer of exchange tokens. HMRC's view is that existing exchange tokens are unlikely to meet the required definition of “stock or marketable securities” or “chargeable securities”. However, each exchange token will need to be considered on its own facts and circumstances in the context of the definitions of “stock or marketable securities” or “chargeable securities”.

- In terms of exchange tokens being given as consideration for purchases of “stock or marketable securities” or “chargeable securities”, SDRT requires that chargeable consideration is “money or money’s worth”. Exchange tokens constitute “money’s worth” and are therefore chargeable for SDRT purposes.
- Stamp Duty Land Tax will not be payable on transfers of exchange tokens as HMRC does not consider such transfers to be land transactions. As with SDRT, chargeable consideration for Stamp Duty Land Tax purposes includes anything given for the transaction that is “money or money’s worth”. Accordingly, if exchange tokens are given as consideration for a land transaction, these would fall within the definition of “money or money’s worth” and be chargeable to Stamp Duty Land Tax.

Money transmission laws and anti-money laundering requirements

Money transmission laws

The principal UK laws relevant to money transmission are the PSRs and the EMRs. Together, the PSRs and EMRs establish a regulatory framework applicable to persons performing payment services (including, for example, money remittance and issuing electronic money) in the UK which includes authorisation, organisational, regulatory capital, safeguarding and conduct of business requirements. Whether this framework applies depends on whether a service involves payment services or electronic money as defined by the PSRs and EMRs, respectively.

Payment services as defined by the PSRs necessarily involve funds. Cryptocurrencies are not considered funds for these purposes. Therefore, products and services involving only cryptocurrency (such as a crypto-to-crypto exchange) will not normally involve payment services. Important exceptions to this are products or services relating to what the FCA Guidance terms “e-money tokens”. Take, for example, a stablecoin structured in a way that means it constitutes electronic money – issuing or providing wallet services in relation to such a stablecoin would be likely to trigger the application of both the PSRs and EMRs.

Conversely, where fiat currency is involved (for example, in the context of a fiat-to-crypto exchange) there will be funds and so further analysis would need to be conducted to determine whether payment services are being provided and, if so, the precise application of the regulatory regime established by the PSRs and EMRs.

Anti-money laundering requirements

UK AML requirements are principally contained in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (“**MLRs**”).

The MLRs implement the Fourth EU Money Laundering Directive in the UK and impose various requirements on businesses that are within their scope, including: the requirement to perform a firm-level AML risk assessment; organisational requirements relating to AML (including systems and controls and record-keeping requirements); customer due diligence obligations when establishing a business relationship with a customer or when transacting above a certain threshold; and ongoing monitoring obligations. The MLRs only apply to those businesses that have been identified as the most vulnerable to the risk of being used for money laundering or terrorist financing.

On 10 January 2020, the MLRs were amended to incorporate the Fifth EU Money Laundering Directive (“**MLD5**”) into UK law. This change brought Cryptoasset Exchange Providers (“**CEPs**”) and Custodian Wallet Providers (“**CWPs**”) within the scope of the MLRs. As such, the MLRs impact upon any person conducting cryptoasset business of

a kind that is captured by the new definitions of CEP or CWP in the UK (including, for example, existing UK authorised financial services firms that carry on relevant cryptoasset business).

For the purposes of the MLRs, CEPs, CWPs and “cryptoassets” are defined as follows:

- **CEP:** “a firm or sole practitioner who by way of business provides one or more of the following services, including where the firm or sole practitioner does so as creator or issuer of any of the cryptoassets involved, when providing such services—
 - (a) exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets,
 - (b) exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or
 - (c) operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets.”
- **CWP:** “a firm or sole practitioner who by way of business provides services to safeguard, or to safeguard and administer—
 - (a) cryptoassets on behalf of its customers, or
 - (b) private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets,when providing such services.”
- **Cryptoasset:** “a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically.”

Significantly, a person may be a CEP or CWP regardless of whether they are otherwise regulated in the UK if they carry on cryptoasset business of a kind that is captured by the new definitions. This means that the new requirements relating to cryptoasset business in the MLRs apply to both regulated and unregulated cryptoasset businesses in the UK. Notably, the definition of a CEP goes beyond the requirements of MLD5, capturing crypto-to-crypto exchange (in addition to crypto-to-fiat exchange). The CEP definition may also capture market participants that would not ordinarily be regarded as exchanges in the strict sense. For example, cryptoasset brokers that buy and sell cryptoassets for their customers or for their own account are likely to be captured by the definition, in addition to exchanges that facilitate interactions between buyers and sellers of cryptoassets. Issuers of cryptoassets may also be captured in certain circumstances.

Typically, providers of non-custodial cryptoasset wallet software will not be captured by the CWP definition.

CEPs and CWPs are required to register with the FCA before carrying on relevant cryptoasset business in the UK. The FCA clarified that existing UK authorised persons (including existing UK banks, investment firms, electronic money institutions and payment services businesses) undertaking relevant cryptoasset business must apply for registration. Registration must be completed via the FCA’s online system, Connect, and applicants must provide a significant amount of information relating to their business and all staff who hold relevant functions to allow the FCA to assess whether or not the applicant is fit and proper. An applicant for registration must provide various information, including: a programme of operations; a business plan; a description of the applicant’s structural organisation; a detailed guide to the applicant’s IT systems and controls; and details of relevant individuals, beneficial owners and close links.

In addition to the ordinary AML requirements that apply generally to businesses within the scope of the MLRs (including CEPs and CWPs), there is a specific additional requirement that a business whose relevant cryptoasset activity does not fall within the scope of the Financial Ombudsman Service or the Financial Services Compensation Scheme must inform its customers of this fact before entering into a relevant business relationship or transaction. There are also specific reporting requirements that apply to CEPs and CWPs (see *Reporting requirements* below).

Relatedly, the Joint Money Laundering Steering Group published sector-specific guidance²⁰ relating to cryptoasset business in July 2020. The guidance clarified the scope of the MLRs in relation to cryptoassets, discussed the money laundering and terrorist financing risks pertinent to the sector, assessed these risks and provided guidance on how CEPs and CWPs might interpret the AML requirements under the MLRs (e.g., customer due diligence, transaction analysis, record keeping and sanctions screening) as would be appropriate to the cryptoasset sector.

Promotion and testing

In November 2018, the FCA established a formal Innovation Division which encompasses the regulator's various initiatives relating to innovation in financial services that it has developed over recent years. Notably in relation to promotion and testing, beneath this umbrella sit:

- The FCA's Regulatory Sandbox, which allows both authorised and unauthorised businesses that meet certain eligibility criteria to test innovative financial services propositions in the market with real consumers. Firms that successfully apply to participate in the Sandbox may benefit from the various Sandbox "tools" that the FCA can deploy to facilitate real-world testing, such as restricted authorisation, individual guidance, informal steers, waivers and no-enforcement action letters.
- The Global Financial Innovation Network, which grew out of the FCA's proposal to create a global Sandbox, seeks to provide a more efficient way for innovative firms to interact with regulators, helping them navigate between countries as they look to scale new ideas. This is for firms wishing to test innovative products, services or business models across more than one jurisdiction.
- The FCA's Innovation Hub, which offers direct support from the FCA to eligible innovative businesses by providing a dedicated contact for innovator businesses that are considering applying for authorisation or a variation of permission, need support when doing so, or do not need to be authorised but could benefit from FCA support.

Ownership and licensing requirements

In the interests of improving legal certainty in this regard, the UK Jurisdiction Taskforce of the UK government's LawTech Delivery Panel ("UKJT") consulted on what it perceived to be the principal issues of legal uncertainty about the status of cryptoassets (including cryptocurrencies) and smart contracts under English private law. These included questions focused on: whether and how cryptoassets can be characterised as personal property; whether cryptoassets are amenable to concepts such as possession and bailment; whether and how security interests may be granted over cryptoassets; and how cryptoassets should be treated for the purposes of UK insolvency law. In a legal statement,²¹ the UKJT concluded that cryptoassets have all the legal characteristics of property and should, as a matter of English legal principle, be treated as property. The statement also concluded that the intangibility of cryptoassets should not disqualify them from being property. Since the publication of

the legal statement (which in itself is not legally binding) it has been adopted by the High Court, which held in one case that cryptoassets were a form of property capable of being the subject of a proprietary injunction.²²

As to licensing requirements, whether or not a person requires authorisation to perform their activities in relation to cryptocurrencies in the UK will depend on whether they are conducting “regulated activities” as defined by FSMA, or payment services/e-money activities that require authorisation under the PSRs or the EMRs. The registration requirement for cryptoasset businesses under the MLRs must also be kept in mind. As noted in *Cryptocurrency regulation* above, a person’s activities in relation to cryptocurrencies may still be subject to UK financial regulation even where the underlying cryptocurrency involved is not a specified investment. A classic example of where this might be the case is that of establishing, operating, marketing or managing a fund that offers exposure to unregulated cryptocurrencies by way of business – this kind of activity may well trigger licensing requirements in the UK. For the time being, cryptocurrencies are also unlikely to be permissible for inclusion in fund products (for example, exchange-traded funds) that require approval from the FCA: it is made clear in the Taskforce Report that the FCA will not authorise or approve the listing of a transferable security or a fund that references exchange tokens unless it has confidence in the integrity of the underlying market and that other regulatory criteria for funds authorisation are met.

Mining

Mining cryptocurrencies is permitted in the UK and, as noted above, there is no bespoke financial regulatory regime for cryptocurrencies in the UK that expressly regulates this activity. Mining of cryptocurrencies is also unlikely to fall within the existing UK financial regulatory perimeter (for example, mining Bitcoin is not currently subject to UK financial regulation).

Border restrictions and declaration

There are currently no border restrictions or requirements to declare cryptocurrency holdings when entering the UK. Individuals carrying cash in excess of EUR 10,000 must declare this to HMRC on entering the UK from a country outside the EU, but cryptocurrencies are not regarded as cash for these purposes.

Reporting requirements

Depending on the nature of the cryptoasset and the business activity in question, general reporting requirements that arise as a result of existing financial regulation (e.g., transaction reporting) or AML legislation (e.g., the requirement to submit suspicious activity reports to the National Crime Agency) could apply in relation to cryptocurrency transactions.

The MLRs now also contain a broad reporting requirement that applies to CEPs and CWPs, under which they must provide to the FCA “such information as the FCA may direct” relating to compliance with the MLRs or that is “otherwise reasonably required by the FCA in connection with the exercise by the FCA of any of its supervisory functions”. Such reports must be made “at such times and in such form, and verified in such manner, as the FCA may direct”. At the time of writing, the FCA is consulting²³ on extending the requirement to provide an annual financial crime report, which currently only applies to certain authorised firms, CEPs and CWPs. Other than this, no guidance has been forthcoming as to how the

FCA intends to utilise its powers in relation to reporting by CEPs and CWPs under the MLRs, and so it remains to be seen what kinds of reports the FCA will require in this regard.

Estate planning and testamentary succession

There are no specific rules as to how cryptocurrencies are treated for the purposes of estate planning and testamentary succession; therefore, the normal relevant legal principles apply. Consequently, cryptocurrencies will fall within the broad definition of property for the purposes of Inheritance Tax,²⁴ and will likely be subject to taxation should a chargeable transfer arise. Prior to death, a testator will need to instruct their personal representative on how to obtain the relevant cryptographic keys and details of the wallet service provider (where relevant), as without such decryption the cryptocurrency will be rendered worthless.

* * *

Endnotes

1. *Cryptoassets Taskforce: Final Report* (26 October 2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf <accessed 12 August 2020>.
2. *Final Report* (n 1), 2.10.
3. *Ibid.*, 2.11.
4. For example, at the time of writing, both the Financial Conduct Authority and Bank of England websites warn that anyone investing in cryptoassets (including cryptocurrencies) should be prepared to lose all of the money invested <https://www.fca.org.uk/consumers/cryptoassets>, <https://www.bankofengland.co.uk/research/digital-currencies> <accessed 12 August 2020>.
5. FCA, *CP19/3: Guidance on Cryptoassets* (23 January 2019) <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> <accessed 12 August 2020>.
6. FCA, *PS19/22: Guidance on Cryptoassets* (31 July 2019) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> <accessed 12 August 2020>.
7. FCA, *CP19/22: Prohibiting the sale to retail clients of investment products that reference cryptoassets* (3 July 2019) <https://www.fca.org.uk/publication/consultation/cp19-22.pdf> <accessed 12 August 2020>.
8. “We have not yet made a decision on whether to introduce CBDC (central bank digital currency).” Bank of England website <https://www.bankofengland.co.uk/research/digital-currencies> <accessed 12 August 2020>.
9. *Central Bank Digital Currency – Opportunities, challenges and design* (March 2020) <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593> <accessed 13 August 2020>.
10. As set out here: <https://www.fca.org.uk/firms/cryptoassets> <accessed 12 August 2020>.
11. <https://www.fca.org.uk/firms/cryptoassets> <accessed 2 August 2020>.
12. This is consistent with the approach taken in the FCA Guidance. See, for example, paragraphs 42, 45, 49 and 65 to 67 of the FCA Guidance: *PS19/22* (n 6), Appendix 1.
13. *PS19/22* (n 6), Appendix 1 41.
14. *Ibid.*, 43 to 44.
15. The FCA maintains a list of UK regulated markets: <https://register.fca.org.uk/search?predefined=RM> <accessed 13 August 2020>.

16. Electronic money does not fall within the definition of transferable securities.
17. HMRC, *Cryptoasset promotions – Consultation* (July 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902891/Cryptoasset_promotions_consultation.pdf <accessed 13 August 2020>.
18. HMRC, *Cryptoassets for individuals* (19 December 2019) <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals> <accessed 12 August 2020>.
19. HMRC, *Cryptoassets for businesses* (20 December 2019) <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses> <accessed 12 August 2020>.
20. JMLSG, Guidance paper on Cryptoasset exchange providers and custodian wallet providers (March 2020) https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-II_-July-2020.pdf <accessed 20 August 2020>.
21. UK Jurisdiction Taskforce, Legal Statement on cryptoassets and smart contracts (November 2019) https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf <accessed 13 August 2020>.
22. *AA v Persons Unknown* [2019] EWHC 3556 (Comm) (17 January 2020).
23. FCA, CP20/17: Extension of Annual Financial Crime Reporting Obligation (24 August 2020) <https://www.fca.org.uk/publication/consultation/cp20-17.pdf> <accessed 25 August 2020>.
24. HMRC, Inheritance Tax Manual: Structure of the charge: what is property? (updated 6 August 2020).

**Stuart Davis****Tel: +44 20 7710 1821 / Email: stuart.davis@lw.com**

Stuart Davis is a partner in the Financial Institutions Industry Group in the firm's London office. Mr. Davis has a wide range of experience advising broker-dealers, investment, retail and private banks, technology companies, market infrastructure providers, investment managers, hedge funds and private equity funds on complex regulatory challenges.

Mr. Davis has considerable experience advising clients on the domestic and cross-border regulatory aspects of cutting-edge FinTech initiatives, including technology innovations in market infrastructure, trading, clearing and settlement, lending (including crowdfunding), payments and regulatory surveillance. Recently, Mr. Davis has advised a number of financial institutions on the impact of MAR and MiFID II on their businesses, and has been heavily involved with assisting institutions on their FX remediation projects, market conduct issues, best execution compliance, CASS compliance, systems and controls, governance, regulatory reform and the implications of Brexit for financial institutions.

**Sam Maxson****Tel: +44 20 7710 1823 / Email: sam.maxson@lw.com**

Sam Maxson is an associate in the London office of Latham & Watkins.

Mr. Maxson regularly advises a wide range of clients (including banks, insurers, investment firms, financial markets infrastructure providers, and technology companies) on all aspects of financial regulation. Mr. Maxson has a particular focus on FinTech and InsurTech, advising both established and emerging businesses on the application of global financial regulation to new and novel uses of technology in finance and insurance. His expertise also extends to the increasingly widespread interest in cryptoassets and “tokenisation” of financial markets.

**Andrew Moyle****Tel: +44 20 7710 1078 / Email: andrew.moyle@lw.com**

Andrew Moyle is the Global Co-Chair of Latham & Watkins' FinTech Industry Group and a partner in the London office. He has more than 20 years of experience in providing commercial legal advice on the structuring, negotiation, implementation, and management of complex technology and outsourcing transactions. Mr. Moyle advises clients ranging from traditional financial institutions to new technology incumbents on the “tech” in FinTech, including on payments and transfers, InsurTech, and virtual currencies.

In his broader technology practice, Mr. Moyle advises clients on commercial contracts and collaborations, cloud computing, outsourcing, digital and disruptive technology, telecommunications technology, and enterprise systems. He regularly engages as the lead legal advisor on outsourcing programs, strategic sourcing functions, and transformation initiatives. In addition to financial services, he also advises clients in leisure, energy, retail, and the natural resource sectors.

Latham & Watkins LLP

99 Bishopsgate, London EC2M 3XF, United Kingdom
Tel: +44 20 7710 1000 / Fax: +44 20 7374 4460 / URL: www.lw.com

USA

Josias N. Dewey
Holland & Knight LLP

Government attitude and definition

In the United States, cryptocurrencies have been the focus of much attention by both Federal and state governments. Within the Federal government, most of the focus has been at the administrative and agency level, including the Securities and Exchange Commission (the “SEC”), the Commodities and Futures Trading Commission (the “CFTC”), the Federal Trade Commission (the “FTC”) and the Department of the Treasury, through the Internal Revenue Service (the “IRS”), the Office of the Comptroller of the Currency (the “OCC”) and the Financial Crimes Enforcement Network (“FinCEN”). While there has been significant engagement by these agencies, little formal rulemaking has occurred. Generally speaking, Federal agencies and policymakers have praised the technology as being an important part of the U.S.’s future infrastructure and the need for the U.S. to maintain a leading role in the technology’s development. Many agencies have acknowledged the risk of overregulating, and cautioned policymakers from passing legislation that would drive investment in the technology overseas.

Several state governments have proposed and/or passed laws affecting cryptocurrencies and blockchain technology, with most of the activity taking place in the legislative branch. There have generally been two approaches to regulation at the state level. Some states have tried to promote the technology by passing very favorable regulations exempting cryptocurrencies from state securities laws and/or money transmission statutes. These states hope to leverage investment in the technology to stimulate local economies and improve public services. One example, Wyoming, has been mentioned as a state seeking a broader impact on its economy. Recently, its legislature passed a bill allowing for the creation of a new type of bank or special purpose depository institution. The new type of bank will act in both a custodial and fiduciary capacity and is meant to allow businesses to hold digital assets safely and legally. The state has been praised for becoming the most crypto-friendly jurisdiction in the country. Another state, Colorado, passed a bipartisan bill exempting cryptocurrencies from state securities regulations. Ohio became the first U.S. state to start accepting taxes in cryptocurrency. Oklahoma introduced a bill authorizing cryptocurrency to be used, offered, sold, exchanged and accepted as an instrument of monetary value within its governmental agencies. On the other hand, Iowa introduced a bill that would prohibit the state and political subdivisions of the state from accepting payment in the form of cryptocurrencies. Authorities in at least 10 other states, like Maryland and Hawaii, have issued warnings about investing in cryptocurrencies. New York, which passed laws once considered restrictive, has eased restrictions for attaining a BitLicense in the hopes of luring back cryptocurrency companies that previously exited the New York market.

There is no uniform definition of “cryptocurrency,” which is often referred to as “virtual currency,” “digital assets,” “digital tokens,” “cryptoassets” or simply “crypto.” While some jurisdictions have attempted to formulate a detailed definition for the asset class, most have wisely opted for broader, more technology-agnostic definitions. Those taking the latter approach will be better positioned to regulate as and when the technology evolves.

Sales regulation

The sale of cryptocurrency is generally only regulated if the sale (i) constitutes the sale of a security under state or Federal law, or (ii) is considered money transmission under state law or conduct otherwise making the person a money services business (“MSB”) under Federal law. In addition, futures, options, swaps and other derivative contracts that make reference to the price of a cryptoasset that constitutes a commodity are subject to regulation by the CFTC under the Commodity Exchange Act. In addition, the CFTC has jurisdiction over attempts to engage in market manipulation with respect to those cryptoassets that are considered commodities. The likelihood of the CFTC asserting its authority to prevent market manipulation is much higher today as a result of both the Chicago Board Options Exchange (“CBOE”) and the Chicago Mercantile Exchange (“CME”) offering futures linked to the price of Bitcoin.

Securities laws

The SEC generally has regulatory authority over the issuance or resale of any token or other digital asset that constitutes a security. Under U.S. law, a security includes “an investment contract,” which has been defined by the U.S. Supreme Court as an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

In determining whether a token or other digital asset is an “investment contract,” both the SEC and the courts look at the substance of the transaction, instead of its form. In 1943, the U.S. Supreme Court determined that “the reach of the [Securities] Act does not stop with the obvious and commonplace. Novel, uncommon, or irregular devices, whatever they appear to be, are also reached if it be proved as matter of fact that they were widely offered or dealt in under terms or courses of dealing which established their character in commerce as ‘investment contracts,’ or as ‘any interest or instrument commonly known as a ‘security’.” *SEC v. C.M. Joiner Leasing Corp.*, 320 U.S. 344, 351 (1943). It has also been said that “Congress’ purpose in enacting the securities laws was to regulate investments, in whatever form they are made and by whatever name they are called.” *Reves v. Ernst & Young*, 494 U.S. 56, 61 (1990).

The SEC has been clear on its position that even if a token issued in an initial coin offering (“ICO”) has “utility,” the token will still be deemed to be a security that is regulated under the Securities Act if it meets elements of the *Howey* test. On February 6, 2018, in written testimony to the U.S. Senate Banking Committee, the Chairman of the SEC stated as follows:

Certain market professionals have attempted to highlight the utility or voucher-like characteristics of their proposed ICOs in an effort to claim that their proposed tokens or coins are not securities. Many of these assertions that the federal securities laws do not apply to a particular ICO appear to elevate form over substance. The rise of these form-based arguments is a disturbing trend that deprives investors of mandatory protections

that clearly are required as a result of the structure of the transaction. Merely calling a token a ‘utility’ token or structuring it to provide some utility does not prevent the token from being a security.

In a more nuanced speech delivered in June 2018, William Hinman, the SEC’s Director of Corporate Finance, stated:

Returning to the ICOs I am seeing, strictly speaking, the token – or coin or whatever the digital information packet is called – all by itself is not a security, just as the orange groves in *Howey* were not. Central to determining whether a security is being sold is how it is being sold and the reasonable expectations of purchasers. When someone buys a housing unit to live in, it is probably not a security. But under certain circumstances, the same asset can be offered and sold in a way that causes investors to have a reasonable expectation of profits based on the efforts of others. For example, if the housing unit is offered with a management contract or other services, it can be a security.

Later in the same speech, Mr. Hinman made clear that a digital token that might initially be sold in a transaction constituting the sale of a security, might thereafter be sold as a non-security where the facts and circumstances have changed over time, such that the *Howey* test is no longer met. While such comments are not official policy of the SEC, they are a good indicator of it.

If a digital asset is determined to be a security, then the issuer must register the security with the SEC or offer it pursuant to an exemption from the registration requirements. For offerings that are being made under a Federal exemption from securities registration, the SEC places fewer restrictions on the sale of securities to “accredited investors.” An individual investor is an “accredited investor” only if he or she (i) is a director or executive officer of the company issuing the securities, (ii) has an individual net worth (or joint net worth with a spouse) that exceeds \$1 million, excluding the value of the investor’s primary residence, (iii) has an individual income that exceeds \$200,000 in each of the two most recent years, and has a reasonable expectation of reaching the same individual income level in the current year, or (iv) has a joint income that exceeds \$300,000 in each of the two most recent years, and has a reasonable expectation of reaching the same joint income level in the current year. See SEC Rule 501(a)(5).

One enforcement action to note is *SEC v. Telegram*. In October 2019, the SEC filed a complaint against Telegram alleging the company had raised \$1.7 billion through the sale of 2.9 billion GRAMS (the company’s native cryptocurrency) to finance its business. GRAMS were to allow customers of the messaging service to use the token as a means of payment for goods and services within the Telegram ecosystem. The SEC sought to enjoin Telegram from delivering the GRAMS it sold, which, using the *Howey* test, the regulator alleged were securities and were not properly registered. In March of 2020, the U.S. District Court for the Southern District of New York issued a preliminary injunction. The SEC argued that the Simple Agreement of Future Tokens (“SAFT”) – mirrored after the commonly used Simple Agreement for Future Equity – and the subsequent resale of GRAMS delivered pursuant to the SAFT, could not be viewed as two isolated phases, but rather should be viewed holistically as a single integrated scheme to issue securities that yield a profit. Ultimately, Telegram abandoned its plan to issue the GRAMS tokens, and agreed to repay the \$1.2 billion to investors and pay an \$18.5 million civil penalty. The SEC’s position could make it more difficult for token issuers to bifurcate between capital-raising activities and the *bona fide* sale of tokens intended to provide some utility other than as an investment.

In addition to Federal securities laws, most states have their own laws, referred to as blue sky laws, which are not always preempted by Federal law. Anyone selling digital assets likely to constitute a security should check with counsel about the applicability of blue sky laws. Of particular importance, there are certain exemptions from registration under Federal law that do not preempt the application of state blue sky laws.

Two other implications for a token constituting a security are (i) the requirement that a person be a broker-dealer licensed with the SEC and a member of the Financial Industry Regulatory Authority (“**FINRA**”) in order to facilitate the sale of securities or to act as a market maker or otherwise constitute a dealer in the asset, and (ii) the asset can only trade on a licensed securities exchange or alternative trading system (“**ATS**”) approved by the SEC. As of August 2020, several exchanges attained approval as an ATS and several firms have been registered as broker-dealers, in each case, with the intent to deal in cryptocurrencies that are considered securities. To date, however, there are only a handful of security tokens actively trading on these ATS platforms. This is likely the result of the difficulties in harmonizing traditional securities laws around the transfer of securities and the notion of a peer-to-peer network that seeks to operate without intermediaries.

Money transmission laws and anti-money laundering requirements

Under the Bank Secrecy Act (the “**BSA**”), FinCEN regulates MSBs. On March 18, 2013, FinCEN issued guidance that stated the following would be considered MSBs: (i) a virtual currency exchange; and (ii) an administrator of a centralized repository of virtual currency who has the authority to both issue and redeem the virtual currency. FinCEN issued guidance that stated as follows: “An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN’s regulations, unless a limitation to or exemption from the definition applies to the person.” See FIN-2013-G001, Application of FinCEN’s Regulations to Persons Administering, Exchanging or Using Virtual Currencies (March 18, 2013).

An MSB that is a money transmitter must conduct a comprehensive risk assessment of its exposure to money laundering and implement an anti-money laundering (“**AML**”) program based on such risk assessment. FinCEN regulations require MSBs to develop, implement, and maintain a written program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. The AML program must: (i) incorporate written policies, procedures and internal controls reasonably designed to assure ongoing compliance; (ii) designate an individual compliance officer responsible for assuring day-to-day compliance with the program and BSA requirements; (iii) provide training for appropriate personnel, which specifically includes training in the detection of suspicious transactions; and (iv) provide for independent review to monitor and maintain an adequate program.

All U.S. persons are prohibited from doing business with foreign nationals who are on the Specially Designated Nationals and Blocked Entities List (“**SDN List**”) of the U.S. Department of the Treasury’s Office of Foreign Assets Control (“**OFAC**”). OFAC provides an updated and searchable version of its SDN List at: sanctionssearch.ofac.treas.gov. OFAC requires all U.S. citizens to “block” (i.e., freeze) the assets of individuals and companies who are engaging in transactions with (i) countries that are subject to U.S. economic sanctions (“blocked countries”), (ii) certain companies and entities that act as agents for such countries (“blocked parties”), and (iii) certain individuals that act as agents

for such countries (“specially designated individuals” or “SDNs”). It is important to have a compliance program in place to avoid (or mitigate) receiving civil and criminal penalties from OFAC for non-compliance. See 31 C.F.R. Part 501 (OFAC Reporting Regulations); OFAC Economic Sanctions Enforcement Guidelines (Nov. 9, 2009).

On February 13, 2018, in response to a letter from Senator Ron Wyden, an official within the Treasury Department issued a correspondence that called into question whether ICO issuers were *de facto* an MSB that was required to register with FinCEN. While there were several flaws in the logic set forth in the letter, it remains an area of concern for anyone considering a token sale. To add more confusion, speaking at a conference on November 19, 2019, FinCEN Director Kenneth Blanco, responding to a question about Facebook’s plan to issue a cryptocurrency pegged to the U.S. dollar, stated that stablecoin issuers and dealers are money transmitters and must follow BSA’s AML laws.

State laws on money transmission vary widely but can generally be grouped into a few categories. Most states define money transmission as including some or all of three types of activities: (1) money transmission; (2) issuing and/or selling payment instruments; and (3) issuing and/or selling stored value. A few states only regulate these activities when “money” is involved, and define money as “a medium of exchange that is authorized or adopted by a domestic or foreign government.” Generally, state money transmission laws apply to any entity that is either located in the state or is located outside of the state (including in a foreign jurisdiction) but does business with residents of the state. A novel solution to the redundancy of attaining state licenses is to become a New York limited purpose trust company. This may seem counterintuitive, as New York has the most onerous money transmitter licensing requirements for cryptocurrency companies, but this type of trust company charter exempts the company from many states’ money transmission laws and requirements, while also providing the ability to conduct a broad range of custody and fiduciary services related to cryptoassets. Nevada and Wyoming have since followed New York and now permit the creation of special purpose depository institutions.

Another tension point for AML laws is the emergence of decentralized finance (“DeFi”). DeFi is the permissionless decentralization version of various traditional financial instruments with a focus on exchanging assets, lending and borrowing and the creation of synthetic assets. For example, Uniswap is a decentralized exchange in the form of two smart contracts hosted on the Ethereum blockchain, as well as a public, open source front-end client. This ultimately allows for anyone with an internet connection to trade many Ethereum-native tokens with other users of the application. Inherent with its open source nature, Uniswap does not have a customer identification vetting process and, in fact, circumventing AML laws is touted as one of Uniswap’s foundational values amongst the cryptocurrency community. As of this writing, there is \$5 billion locked into DeFi applications.

Taxation

In March 2014, the IRS declared that “virtual currency,” such as Bitcoin and other cryptocurrency, will be taxed by the IRS as “property” and not currency. See IRS Notice 2014-21, Guidance on Virtual Currency (March 25, 2014). Consequently, every individual or business that owns cryptocurrency will generally need to, among other things, (i) keep detailed records of cryptocurrency purchases and sales, (ii) pay taxes on any gains that may have been made upon the sale of cryptocurrency for cash, (iii) pay taxes on any gains that may have been made upon the purchase of a good or service with cryptocurrency, and (iv) pay taxes on the fair market value of any mined cryptocurrency, as of the date of receipt.

For an individual filing a Federal income tax return, the gains or losses from a sale of virtual currency that was held as a “capital asset” (i.e., for investment purposes) are reported on (i) Schedule D of IRS Form 1040, and (ii) IRS Form 8949 (Sales and Other Dispositions of Capital Assets). Any realized gains on virtual currency held for more than one year as a capital asset by an individual are subject to capital gains tax rates. Any realized gains on virtual currency held for one year or less as a capital asset by an individual are subject to ordinary income tax rates. The IRS requires, on Form 8949, for each virtual currency transaction, the following information be disclosed: (i) a description of the amount and type of virtual currency sold; (ii) the date acquired; (iii) the date the virtual currency was sold; (iv) the amount of proceeds from the sale; (v) the cost (or other basis); and (vi) the amount of the gain or loss. It should be noted that the record-keeping requirements of IRS Form 8949 can be particularly onerous for those who have used cryptocurrency to make numerous small purchases of goods or services throughout the year.

For transactions completed on or after January 1, 2018, the Internal Revenue Code now prohibits the use of Section 1031(a) for cryptocurrency transactions, and requires a taxpayer to recognize taxable gain or loss at the time that any cryptocurrency is converted into another cryptocurrency. Section 13303 of P.L. 115-97 (the tax act signed into law on December 22, 2017) changes Section 1031(a) to state as follows: “No gain or loss shall be recognized on the exchange of real property held for productive use in a trade or business or for investment if such real property is exchanged solely for real property of like kind which is to be held either for productive use in a trade or business or for investment.”

For transactions completed on or prior to December 31, 2017, the IRS has not issued any guidance on whether different cryptocurrencies are “property of like kind” that would qualify for non-recognition of gain under Section 1031(a). Generally speaking, exchanges between different cryptocurrencies are usually done by either (i) a simultaneous swap of one cryptocurrency for another, or (ii) a deferred exchange, in which one cryptocurrency is sold for cash, followed by the purchase for cash, of a different cryptocurrency.

For transactions completed on or prior to December 31, 2017, Section 1031(a)(1) of the Internal Revenue Code states the following: “No gain or loss shall be recognized on the exchange of property held for productive use in a trade or business or for investment if such property is exchanged solely for property of like kind which is to be held either for productive use in a trade or business or for investment.” In 26 C.F.R. 1.1031(a)-2(b), “like kind” is defined as follows: “As used in section 1031(a), the words like kind have reference to the nature or character of the property and not to its grade or quality. One kind or class of property may not, under that section, be exchanged for property of a different kind or class.” It should be noted that, in order to attempt to utilize the tax treatment of Section 1031(a) for transactions done on or prior to December 31, 2017, (i) each transaction must comply with certain requirements set forth in IRS regulations (such as the use, in certain instances, of a “qualified intermediary”), and (ii) the taxpayer must file a Form 8824 with the IRS.

There is a risk that the IRS could use its prior revenue rulings on gold bullion as a basis for taking the position that, for transactions completed on or prior to December 31, 2017, different cryptocurrencies are not “property of like kind” under Section 1031(a). In Rev. Rul. 82-166 (October 4, 1982), the IRS ruled that an exchange of gold bullion for silver bullion does not qualify for non-recognition of gain under Section 1031(a). The IRS stated: “Although the metals have some similar qualities and uses, silver and gold are intrinsically different metals and primarily are used in different ways. Silver is essentially an industrial commodity. Gold is primarily utilized as an investment in itself. An investment in one of the

metals is fundamentally different from an investment in the other metal. Therefore, the silver bullion and the gold bullion are not property of like kind.” The IRS also stated in Rev. Rul. 79-143 (January 5, 1979) that an exchange of \$20 U.S. gold numismatic-type coins and South African Krugerrand gold coins does not qualify for non-recognition of gain under Section 1031(a). The IRS stated: “The bullion-type coins, unlike the numismatic-type coins, represent an investment in gold on world markets rather than in the coins themselves. Therefore, the bullion-type coins and the numismatic-type coins are not property of like kind.”

Promotion and testing

Arizona became the first state in the U.S. to adopt a “regulatory sandbox” to shepherd the development of new emerging industries like fintech, blockchain and cryptocurrencies within its borders. The law grants regulatory relief for innovators in these sectors who desire to bring new products to market within the state. Under the program, companies are able to test their products for up to two years and serve as many as 10,000 customers before needing to apply for formal licensure. Other states have since followed suit and created similar programs including Hawaii, Kentucky, Nevada, Utah, Vermont and Wyoming.

Ownership and licensing requirements

Cryptocurrency fund managers that invest in cryptocurrency futures contracts, as opposed to “spot transactions” in cryptocurrencies, are required to register as a commodity trading advisor (“CTA”) and commodity pool operator (“CPO”) with the CFTC and with the National Futures Association (“NFA”), or satisfy an exemption. Also, because of additions to the Dodd-Frank Act, cryptocurrency hedge fund managers that use leverage or margin would also need to register with the CFTC and NFA. The Dodd-Frank Act amended the Commodities Act to add new authority over certain leveraged, margined, or financed retail commodity transactions. The CFTC exercised this jurisdiction in an action against BFXNA INC. d/b/a BITFINEX in 2016. Fund managers should be cautious when using margin/leverage as it may require them to register as a CTA and CPO with the CFTC and register with the NFA.

The Investment Company Act of 1940 (the “**Company Act**”), the Investment Advisers Act of 1940 (the “**Advisers Act**”), as well as state investment advisor laws, impose regulations on investment funds that invest in securities. The Company Act generally requires investment companies to register with the SEC as mutual funds unless they meet an exemption. Cryptocurrency funds, and hedge funds generally, can be structured under one of two exemptions from registration under the Company Act. Section 3(c)(1) allows a fund to have up to 100 investors. Alternatively, Section 3(c)(7) allows a fund to have an unlimited number of investors (but practically it should be limited to 2,000 to avoid being deemed a publicly traded partnership under the Securities Exchange Act) but requires a significantly higher net-worth suitability requirement for each investor (roughly \$5 million for individuals, \$25 million for entities). As a general rule, most startup funds are structured as 3(c)(1) funds because of the lower investor suitability requirements.

Until the SEC provides more guidance on classifying individual cryptocurrencies as securities or commodities, the likelihood of many cryptocurrencies being deemed securities is high. As such, we recommend that cryptocurrency funds that invest in anything other than Bitcoin, Ether, Litecoin, and the handful of other clearly commodity coins, comply with the Company Act preemptively. For most startup funds, this would mean limiting investors within a given fund to less than 100 beneficial owners.

Regardless of whether a startup cryptocurrency fund manager is required to register as a CPO/CTA with the CFTC under the Commodities Act, register or seek exemption from the SEC as an investment advisor (under the Advisers Act), or investment company (under the Company Act), every cryptocurrency fund manager will be subject to the fraud provisions of the CFTC and/or the SEC. In September 2017, the CFTC announced its first anti-fraud enforcement action involving Bitcoin. These anti-fraud actions can be taken by the SEC and CFTC regardless of the cryptocurrency fund's exempt status.

In July of 2020, the OCC affirmed in an interpretive letter that national banks and savings associations can provide custody services for cryptocurrency. The letter noted that banks can also provide related services such as cryptocurrency-fiat exchanges, transaction settlement, trade execution, valuation, tax services and reporting. The effort supplements a patchwork of state regulation and guidance that to date has encouraged only a select few national banks and financial services companies to embrace cryptocurrency (*see above: Money transmission laws and anti-money laundering requirements*). While the OCC agreed that underlying keys to a unit of cryptocurrency are essentially irreplaceable if lost, it said that banks could be a part of the solution by offering more secure storage services compared to existing options.

Mining

The general rule of thumb regarding Bitcoin mining remains relatively straightforward. If you are able to own and use cryptocurrency where you live, you should also be able to mine cryptocurrency in that location as well. If owning cryptocurrency is illegal where you live, mining is most likely also illegal. There are few, if any, jurisdictions in the U.S. where possession of cryptocurrency is illegal. Plattsburgh, New York, however, is likely the only city in the U.S. to impose a ban (temporary) on cryptocurrency mining. Also, the U.S. Marine Corps banned crypto mining apps from all government-issued mobile devices.

Border restrictions and declaration

A group of U.S. lawmakers have proposed a requirement that individuals declare their cryptocurrency holdings when entering the U.S., but to date no such requirement has gone into effect.

Reporting requirements

We are not aware of any broadly applicable reporting requirements specific to cryptocurrency in the U.S.

Estate planning and testamentary succession

Cryptocurrency, such as Bitcoin, has value and therefore is increasingly likely to become an estate asset. While there are few, if any, laws specific to cryptocurrency, due to the nature of cryptocurrencies, typical wills and revocable living trusts may not be well suited to efficiently transfer this new type of asset. Consequently, new estate planning questions and clauses may be needed.

While cryptocurrency is not sufficiently mature to allow existing legal structures to promulgate a complete set of rules and regulations, cryptocurrency's technological character allows estate planning to protect the intent of clients holding cryptocurrency. However, the lack of statutory structure necessitates proactive steps. Accordingly, someone who wants

greater certainty of bequeathing cryptocurrency to their heirs will need to provide specific and detailed written instructions in their estate planning documents. The information they will need to include will depend upon the type of virtual currency wallet that they have.

There is wide range of cryptocurrency wallets that are available at this time. The current types of cryptocurrency wallets include: (i) a single device software wallet in which you hold the private keys (example: bitpay wallet); (ii) a multiple device web wallet in which you hold the private keys (example: blockchain wallet); (iii) a multiple device web wallet in which you do not hold the private keys (example: coinbase wallet); (iv) a USB hardware dongle wallet in which you hold the private keys (example: trezor wallet); and (v) a “paper wallet” in which the private keys and public keys are written down (which can be later loaded into a software wallet of your choice to be spent).

The instructions that you provide in a will (for your personal representative) or in a declaration of trust (for the successor trustee of a revocable living trust) should be written in a manner that is easy to understand for individuals who are not familiar with cryptocurrency. For example, in the case of a single device software wallet in which you hold the private keys, instructions could include (i) a description of the name and version of the wallet software, (ii) a description of the name and version of the operating software system of the wallet device (i.e., iOS, Android, MacOS, Windows or Linux), (iii) a description of the types of virtual currency held by the wallet, (iv) either the long-form private and public keys for the wallet or the 12-word “seed” BIP39 or BIP44 recovery phrase for the wallet, and (v) step-by-step instructions (which may include screenshots) showing how the wallet can be restored onto a new device, if the current wallet device cannot be accessed.

As transfers from a Bitcoin wallet and most other wallets are irrevocable, private key information about cryptocurrency accounts will need to be kept in a secure manner. Security can be enhanced by storing the private key information in a safe-deposit box or vault, which could only be accessed after the holder’s death by the personal representative designated in their will (or the successor trustee designated in their revocable living trust).

**Josias N. Dewey****Tel: +1 305 374 8500 / Email: joe.dewey@hkllaw.com**

Josias “Joe” N. Dewey is a finance and real estate attorney with the law firm of Holland & Knight LLP. Mr. Dewey also serves as the firm’s Innovation Partner and is a member of the firm’s Practice and Operations Committee. In addition, Mr. Dewey co-chairs the firm’s Technology and Telecommunication Industry Sector Group. Mr. Dewey regularly represents a diverse group of banks and other financial institutions, from large international banks to local community banks. In addition to his traditional finance practice, a significant portion of Mr. Dewey’s practice involves blockchain technology. Mr. Dewey has served in various court-appointed capacities in connection with enforcement actions brought by the U.S. Securities and Exchange Commission, including federal receiver, independent intermediary and Fair Fund distribution agent. Some of these engagements have involved extensive asset recovery efforts where the principal assets were digital assets, such as bitcoin and ether. Mr. Dewey is the co-author of the book, *“The Blockchain: A Guide for Legal and Business Professionals”*.

Holland & Knight LLP

701 Brickell Avenue, Suite 3300, Miami, FL 33131, USA
Tel: +1 305 374 8500 / Fax: +1 305 789 7799 / URL: www.hkllaw.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

AI, Machine Learning & Big Data

Banking Regulation

Bribery & Corruption

Cartels

Corporate Tax

Employment & Labour Law

Energy

Fintech

Fund Finance

Initial Public Offerings

International Arbitration

Litigation & Dispute Resolution

Merger Control

Mergers & Acquisitions

Pricing & Reimbursement