Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Virtual Currencies and Financial Crime

Challenges and Opportunities

David Carlisle

Virtual Currencies and Financial Crime

Challenges and Opportunities

David Carlisle

RUSI Occasional Paper, March 2017

Royal United Services Institute
for Defence and Security Studies

185 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 185 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2017 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, March 2017. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

Printed in the UK by Stephen Austin and Sons, Ltd.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

The author thanks Tom Keatinge, Inês Sofia de Oliveira and Florence Keen of RUSI's Centre for Financial Crime and Security Studies (CFCS) for their encouragement and support in preparing this paper. He also thanks the many experts with whom he consulted during the writing of this report for generously offering their time, knowledge and advice. He is especially grateful to Joseph Mari, Joe Ciccolo, Emma Hardaker and Mara Wesseling for providing views, comments and feedback.

Executive Summary

THE RAPID RISE of Bitcoin[1] has prompted extensive discussion about the nexus between virtual currencies (VCs) and financial crime. The issue is a timely one for EU member states. Under the EU's 5th Money Laundering Directive (MLD)[2], still under negotiation at the time of this paper's publication, member states will be required to bring certain VC service providers under their anti-money laundering/counter-terrorist finance (AML/CTF) regulation, with a target implementation date of 26 June 2017. The measure forms part of efforts to strengthen the region's AML/CTF defences following the November 2015 terrorist attacks in Paris.

The general public has typically reacted with mystification to Bitcoin and other VCs, or tradable digital representations of value developed by private actors and with no status as legal tender. Press reporting often focuses on instances of criminals using VCs, adding concern to the confusion. Some governments have gone as far as to ban all dealings in VCs.

VCs pose a number of financial crime risks. In particular, they offer rapid international transaction settlement and a greater degree of anonymity around users' identities than many other established electronic payment methods; and they do so without involving banks or other powerful intermediaries in payment processing. A payment method that affords secrecy, operates outside the established financial system and facilitates speedy international payments provides obvious attractions to global criminals.

However, the story of VCs is not one of unhindered criminality. Far from it. VCs have a number of legitimate and beneficial applications. Speedier, more cost-efficient transaction settlement could create a nimbler financial system better suited to today's global economy. VCs and related technology could help to deliver dynamic, mobile financial services to a greater number of people – such as those in developing countries who have limited or no access to banks. In addition, cryptocurrencies, the most widely-known type of VC, are just one innovation in a broader development towards decentralised computing that could have far-reaching societal consequences.

It is true that criminals – and in particular cybercriminals, who have recently found significant success in Bitcoin as a form of ransom payment – have exploited VCs. But open source reporting

1. This paper follows standard practice of using an initial capital to describe Bitcoin as a network, payment platform or protocol; it uses lowercase to refer to units of bitcoin as a currency.
2. The 5th Money Laundering Directive is a common name used to refer to a series of amendments to the EU's 4th Money Laundering Directive, and which include measures related to virtual currencies. At the time of writing, the EU Parliament was still negotiating changes to the the 5th Money Laundering Directive, with the expectation that member states will be required to undertake implementation of the new measures by 26 June 2017. A recent copy can be viewed at <http://www.bakermckenzie.com/-/media/files/insight/publications/2016/12/report_external_thirdpresidencycompromise_nov16.pdf?la=en>, accessed 21 February 2017.

suggests that more traditional criminal organisations that engage in large scale money laundering are still in the early stages of adapting to Bitcoin and other cryptocurrencies and do not appear to use them on a widespread scale. It is unclear whether money launderers will adopt them more widely. While terrorist organisations such as Daesh (also known as the Islamic State of Iraq and Syria, or ISIS) are interested in using VCs, reports that terrorists are actively using them are generally unconfirmed and anecdotal. There is no indication that VCs played a role in funding the Paris attacks that prompted the EU's latest measures. While VCs could grow as a tool of criminal and terrorist finance, that risk is still far from fully realised.

Indeed, VCs have several characteristics that can limit their usefulness in financial crime. Their prices are frequently volatile, they are still a small part of the global financial system and they require a technological adeptness that some criminal organisations are just acquiring. More importantly, despite a common misperception, VCs are not uniformly anonymous. Bitcoin, by far the most widely used of cryptocurrencies, relies on a ledger system – the blockchain – that is publicly available and allows for a series of transactions to be traced from end to end. Law enforcement agencies are able to use a variety of new forensic techniques and tools alongside their traditional investigative methods to analyse and follow illicit flows of Bitcoin in support of criminal investigations.

This combination of technological potential and evolving financial crime risk presents a challenge. Viewing VCs purely through the lens of their security implications is problematic and unhelpful. Officials worry about the unknown consequences of new technology; but governments may over-regulate or mis-regulate in ways that can hinder new financial innovations if they act hastily, before the extent of a new technology's innovative potential has been fully explored. Governments are taking a number of initial steps to meet the challenge of VCs, with varying degrees of success.

Governments are not the only stakeholders. As Bitcoin has grown, the communities that surround decentralised VCs – and which include developers, miners, exchanges, wallet providers and traders – have evolved into a full-fledged, if still young, industry. As they work to promote the widespread adoption and use of VCs, a growing number of companies in the VC industry accept that they have a role in the fight against financial crime. VC service providers in the UK and across the EU will soon join banks and other financial sector participants in implementing AML/CTF regulation. Consequently, VC service providers will have a responsibility to be partners with the public sector in ensuring a robust AML/CTF regime. However, the established AML/CTF framework and the VC industry are not necessarily a harmonious fit; indeed, certain aspects of VC networks – such as certain VC wallet providers, which the EU is set to regulate under the 5th MLD – rely on operating models that often do not resemble those of traditional financial institutions for which the existing AML/CTF regime was designed.

Banks and other existing financial institutions also have a stake in the matter. Banks often view VC start-ups with scepticism, as disruptors carrying significant risks. VC start-ups, for their part, see banks as hindering innovation. How the traditional financial sector and the VC industry interact will be critical for the future of VCs and other disruptive financial technology.

This paper examines the financial crime risks involving VCs (with a particular focus on decentralised cryptocurrencies), the challenges that come with attempting to address those risks, and considers the implications for key stakeholders. It recommends the following high-level principles for governments, the VC industry and established financial sector participants.

A Forward-Looking, Adaptive Approach

Governments must avoid the temptation to over-react and mis-regulate. They should not rely on an outdated set of AML/CTF approaches. Rather, governments should study VCs to understand how to combat future financial crimes, while also allowing the technology room to evolve so that its potential benefits may be explored fully.

Legal and regulatory frameworks around VCs should be clear in their intentions and scope, but sufficiently dynamic to enable responsiveness to technological change. Because certain aspects of decentralised VC networks do not fit comfortably within the framework of AML/CTF regulation, merely enacting restrictions on the use of VCs, or expanding the application of AML/CTF regulation beyond VC exchanges, is unlikely to be helpful if founded in outdated conceptual frameworks.

Instead, governments should take a longer view and consider what new legal and regulatory tools and approaches may be required to make global AML/CTF efforts better equipped to deal with twenty-first century finance. This could include governments using a combination of traditional AML/CTF regulation on a limited number of actors – such as VC exchanges – while also enabling dynamic frameworks – such as the use of self-regulation or regulatory sandbox intitiatives – to evolve around other system participants, such as certain VC wallet providers, with the ultimate aim of determining, with time, whether new regulatory approaches might be most appropriate. An adaptive response need not be complacent; stakeholders can take an approach that ensures vigilance that is proportionate to risk.

A Global View

VCs are still in their infancy, so governments are undertaking a range of approaches. Because cryptocurrencies and related technology offer decentralised transaction platforms, the international community should, with time, harmonise its approach if the benefits of VCs are to be realised and the risks managed in a proportionate manner. A harmonised approach can help to ensure that the legitimate use of VCs is not inadvertently disrupted. International efforts should include sharing information and developing detailed typologies of the use of VCs in financial crime schemes to enable better understanding of risks.

Partnership and Exchange

To achieve the previous aim, governments, the VC industry and the established financial sector should collaborate closely. The formation of public–private partnerships is essential to determine how risks can be mitigated without hindering innovation. Stakeholders should leverage their

strengths for mutual benefit: governments can provide the private sector with information on criminal typologies; the VC industry can provide detailed analysis of trends they observe; and banks can offer valuable lessons learned from their experience in AML/CTF compliance.

Innovative Solutions

All stakeholders, and the VC industry in particular, should harness the potential of this new technology to combat financial crime. Start-ups should continue to apply their entrepreneurial mindset to developing sophisticated tools for detecting illicit activity involving VCs, while also addressing legitimate privacy concerns. Public–private partnerships can enable funding of these efforts.

Introduction

BITCOIN'S HISTORY ILLUSTRATES the complexity of financial crime issues surrounding VCs. In October 2008, an unknown individual or individuals using the pseudonym 'Satoshi Nakamoto' published a paper online setting out the idea for Bitcoin.[1] Nakamoto's proposal provided for a fully 'peer-to-peer' payment network – that is, users could trade the 'currency' directly, without the interference or participation of any government, financial sector intermediary or third-party administrator. In this sense, the Bitcoin network bears some resemblance to an open platform website such as Wikipedia.[2] Bitcoin relies not on a central authority, but rather on the active engagement of its network participants to sustain it.

The concept had long been part of the ultra-libertarian 'cypherpunk' movement of technologists who aimed to undermine the influence of government and large banks over the financial system by putting financial tools directly in the hands of individuals. Other developers had attempted to create viable decentralised VCs, but Nakamoto was the first to develop one that proved viable on a significant scale.[3]

VCs take a number of forms.[4] The most widely known are cryptocurrencies, such as Bitcoin, which are designed to function as a substitute to government-issued cash. Cryptocurrencies rely on decentralised networks to facilitate transactions among users in a particular unit of account. As such, there is no central administrator issuing Bitcoin in the way that a government issues and backs fiat currencies (currency that a government has declared to be legal tender); rather, a network protocol and cryptographic solutions enable users to exchange their bitcoins with one another in a manner that ensures consensus about the authenticity of transactions. Cryptocurrencies resemble cash in that they are 'bearer' instruments: whoever possesses a unit of a cryptocurrency is considered to be its owner, just as a person holding paper cash is assumed to be its owner. However, rather than physical possession, a string of digital records indicates which network user 'holds' the particular unit of cryptocurrency.

---

1. Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', October 2008.
2. Chang Jia, 'Wikipedia and Bitcoin: From Self-Organization to Specialization', *Bitcoin Magazine*, 29 October 2013.
3. Paul Vigna and Michael J Casey, *Cryptocurrency: The Future of Money?* (London: Vintage, 2016), pp. 42–43.
4. The terms 'digital currency' and 'VC' are often used interchangeably. This paper treats them distinctly, in keeping with guidance established by the Financial Action Task Force (FATF). 'Digital currency' refers here to any digital representation of value, including both government-issued and privately developed currency. VCs, conversely, are not government-issued or government-backed. This paper employs the term VC to refer generally to the range of VC schemes that exist, but specifies with terms such as 'centralised VC', 'decentralised VC' and 'cryptocurrency' where appropriate.

Cryptocurrencies allow users to engage in speedy electronic payments, but without banks or other financial institutions settling transactions. Credit cards, wire transfers and other transaction methods require intermediary companies to process them, resulting in high fees and delayed processing times. Cryptocurrencies, by contrast, enable rapid, disintermediated settlement at a generally lower cost than well-established payment methods.[5]

Importantly, cryptocurrencies such as Bitcoin are also convertible. An ever-growing number of start-up VC exchanges exist online, where users can exchange their fiat money for VCs, and vice versa. Users obtain an electronic 'wallet' for storing VCs – held on their computer, the Cloud or on a mobile device – and then have several options: to transfer their VC to another wallet; to purchase goods or services from a vendor that accepts the VC; to exchange VC for cash at a VC ATM; or to hold the VC as a speculative instrument, trading it as its value fluctuates against fiat currencies.

Initially, only a very small number of tech enthusiasts traded Bitcoin. In 2010, the first Bitcoin purchase of a real good occurred when a user purchased pizzas. There are now more than 15 million total bitcoins in circulation. More than 150 million total Bitcoin transactions have been undertaken to date, with over 250,000 transactions a day (by contrast, the total volume of all non-cash payments worldwide exceeds 1 billion per day).[6] One major Bitcoin wallet provider – Blockchain[7] – manages more than 12 million wallets, which represents a twelve-fold increase since 2014. The bulk of dealing in Bitcoin is speculative; most traders deal in Bitcoin hoping to profit on its movements against fiat currencies[8] – a fact that leads some to question its value as 'currency'. Volatility in its price and a lack of trust and knowledge about Bitcoin are among a number of factors that limit its utility among the general public. However, standard retail usage has grown since Bitcoin's founding, even if it is still a very small component of wider economic activity. Globally, more than 100,000 merchants accept Bitcoin, and approximately 1,000 Bitcoin ATMs are in operation worldwide, a ten-fold increase in two years.[9]

Cryptocurrencies other than Bitcoin are called 'altcoins', of which there are at least several hundred. Among the more well known are Ethereum, Ripple, Litecoin, Ethereum Classic, Monero, Dash and Zcash. The total present market capitalisation of cryptocurrencies at the time of this paper's publication is an estimated $24 billion, with approximately 70% of that comprised of

5. Dan Blystone, 'Bitcoin Transactions Vs. Credit Card Transactions', *Investopedia*, 22 April 2015. As Blystone notes, credit card transactions typically result in fees ranging from 0.5% to 5%. Bitcoin wallet providers and Bitcoin-accepting merchants may charge fees, but these are generally very low, less than 0.5%. See also, *Tablets and Tech*, 'Bitcoin Vs. Visa – Transaction Fees', 25 July 2014.
6. For daily Bitcoin transaction volumes, see <http://www.coindesk.com/data/bitcoin-daily-transactions/>, accessed 21 February 2017; for total global non-cash payment volumes, see <https://www.worldpaymentsreport.com/#non-cash-payments-content>, accessed 21 February 2017.
7. Note that the company Blockchain, which is a provider of Bitcoin wallets, is a commercial entity and is distinct from the blockchain ledger system that underpins the Bitcoin network, and which is discussed in further detail below.
8. Nathaniel Popper, 'How China took Center Stage in Bitcoin's Civil War', *New York Times*, 29 June 2016.
9. Coin ATM Radar, 'Bitcoin ATMs by Manufacturer Details', <https://coinatmradar.com/chart/bitcoin-atm-location-growth/>, accessed 8 December 2016.

Bitcoin.[10] It is due to this market dominance that Bitcoin is at the centre of discussions about cryptocurrencies.

These figures do fully not capture the implications of this new technology. The Bitcoin network represents a tremendous feat of decentralised computing. Bitcoin is sustained by computing power 500 times more powerful than Google and significantly more powerful than the world's largest supercomputers – all generated across a diffuse, unofficial network that is driven entirely by its voluntary participants.[11] Bitcoin represents the ability of new, decentralising technologies to upend models of social interaction.

Bitcoin owes its success over other attempts to develop decentralised payment schemes to Nakamoto's innovative approach for harnessing two technological solutions: the blockchain and mining. The blockchain is part of Bitcoin's software protocol and acts as the network's accounting system. It is a 'distributed ledger technology' (DLT) – a scheme that enables 'a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, and/or institutions'.[12] In the absence of a reliable third-party arbiter, Bitcoin requires a means of establishing a coherent picture of intra-network activity. The blockchain serves this function. It records new transactions as blocks and links them to previous transactions, ensuring a chronological history of all activity undertaken within the network. It contains a complete history of all Bitcoin transactions ever made. The network is entirely public, and participants rely on identical copies of the ledger – the blockchain is maintained on a multitude of computers across the network, or 'nodes', rather than by any single record-keeper. As an accounting device for a diffuse network, the blockchain marks a significant innovation to the double-entry book-keeping methods[13] on which central banks and the formal financial sector have relied for centuries. Many observers therefore see the disruptive potential of the underlying technology as more important than Bitcoin as a currency. Governments are keen to harness the promise of DLT to make financial services more efficient, and are exploring the potential of DLT to enhance other public sector services as well, such as in recording transfers of property ownership and for recordkeeping in healthcare.

Nakamoto also aimed to maintain privacy in the Bitcoin network. Ideally, one individual transferring cryptocurrency to another should be as undetectable as those same individuals handing cash to one another on the street. Nakamoto's solution was to identify users on the blockchain, not by their actual names, but by alphanumeric 'public keys' associated with their wallet. For example, the wallet address for the controversial WikiLeaks website appears on the

10. Coin Market Cap, 'CryptoCurrency Market Capitalizations', <http://coinmarketcap.com/>, accessed 8 December 2016.
11. Reggie Middleton, 'Bitcoin's Computing Network is More Powerful than 525 Googles and 10,000 Banks!', *Zero Hedge*, 19 November 2015; *The Economist*, 'How Bitcoin Mining Works', 20 January 2015.
12. Blockchain Technology, 'Blockchain Technology Explained', <http://www.blockchaintechnologies.com/blockchain-definition>, accessed 9 February 2017.
13. In double-entry book-keeping, every transaction involves offsetting debit and credits on each account involved. If customers at two separate banks transact, each bank records the transaction as either a debit or credit on the separate accounts they hold for their respective customers. Bitcoin, by contrast, involves only a single, shared ledger.

blockchain as 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v.[14] But even when using alphanumeric identification, this public recordkeeping system provides a point of tension to the privacy aims of the cypherpunks.

Nakamoto recognised that having a ledger was not sufficient to drive a network alone. The blockchain organises data from across the Bitcoin network, but to have value, bitcoins could not just be made freely available; people required an incentive to participate. And Nakamoto needed a mechanism to build consensus about the validity of information recorded on the blockchain. The solution to these problems is 'mining'.

When two Bitcoin users wish to transact, a message is broadcast to the Bitcoin network. Before the transaction is recorded on the blockchain, a participant in the network must validate the transaction and group it into a block with other pending transactions. Computers in the network then race to calculate, or 'mine', a solution to a cryptographic puzzle that allows the block to be linked to a previously confirmed block. Once a miner finds a solution, other network participants check the accuracy of their work – creating consensus that the transactions are authentic and can be added to the blockchain.[15] This process helps to secure the Bitcoin network by enabling the blockchain to act as an immutable record: altering transactional information stored on the blockchain would require duplicating the entire mining process from when Bitcoin was created – an impractical feat.

Mining requires significant computing power, so Nakamoto developed an algorithm to reward miners for their service to the network: miners receive bitcoins whenever they confirm a block. Mining has since become an enormous business, largely centred in China, and significant amounts of energy go into making Bitcoin functional on the scale it has achieved.[16]

Bitcoin's success as a technological feat, however impressive, quickly generated controversy. The first major incident was the US law enforcement crackdown on Silk Road, an online black marketplace operating on The Onion Router (Tor) network, an encrypted web service that conceals its users' identities. Founded in 2011, Silk Road facilitated Bitcoin transactions, primarily for drugs, but also for stolen goods, forged documents and hacking services.[17] In 2013, the FBI arrested Ross Ulbricht, Silk Road's founder, and charged him with money laundering and other crimes. In May 2015, Ulbricht was sentenced to life in prison without the possibility of parole. The Silk Road case stoked a popular view that cryptocurrencies were nothing more than a tool for criminals operating in complete anonymity in the darkest realms of the web. Politicians seized on the case and in 2014 US Senator Joe Manchin advocated that the US ban all Bitcoin trading.[18]

14. Blockchain, <https://blockchain.info/address/1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v>, accessed 8 December 2016.
15. This process of building consensus by demonstrating that sufficient computational effort has gone into solving a cryptographic puzzle is referred to as a 'proof-of-work' algorithm.
16. *The Economist*, 'Bitcoin: The Magic of Mining', 10 January 2015.
17. Vigna and Casey, *Cryptocurrency: The Future of Money?*, pp. 84–87.
18. Joe Manchin, 'Manchin Demands Federal Regulators Ban Bitcoin', press release, 26 February 2014.

While the Silk Road case revealed a risk, it also demonstrated an irony: for all its supposed secrecy, Bitcoin was in fact highly traceable. Once the FBI established that a particular Silk Road user was using specific public wallet addresses, it could trace that individual's transaction history on the blockchain.[19] The cypherpunks had envisioned cryptocurrencies as a means for engaging in commerce outside of government view, yet the blockchain offered a fully public money trail of Bitcoin transactions for law enforcement to use in its investigations.

The second major incident that threatened Bitcoin's reputation involved Mt. Gox, a Bitcoin exchange based in Tokyo. In 2014, Mt. Gox, which at one point facilitated as much as 80% of all Bitcoin trades, announced that it had lost approximately $450 million-worth of its users' bitcoins.[20] Whether this was the result of an external hack or possible theft by Mt. Gox's staff is still unclear. But the loss drove the price of Bitcoin down precipitously overnight, required the exchange to be closed and led to its bankruptcy.[21] Set alongside an earlier loss of bitcoin at Mt. Gox in 2011, this incident created an impression that Bitcoin was operating in a generally lawless environment that could imperil its users.

Despite these high-profile cases, many governments in the UK, Europe, the US and elsewhere have adopted a 'wait-and-see' approach to VCs. The US has not banned Bitcoin. Although some countries continue to ban VCs, most jurisdictions are seeking solutions that recognise VCs are here to stay, while allowing for risk management.

Intelligence and law enforcement agencies are still building a picture of the use of VCs in financial crime. While evidence exists that established criminal and terrorist groups are beginning to use VCs, these groups have other reliable financing methods that may obviate their need to rely on VCs on a large scale in the near term. The total value of VCs that criminals use are still minute compared to the volumes of illicit funds that flow using more well-established payment methods, such as cash or credit cards. Yet the prospect that traditional criminal and terrorist networks could adopt VCs on a larger scale is real and represents a concern to security personnel.

Where law enforcement agencies do have more immediate concerns about the illicit use of VCs, it is with the rapidly growing occurrence of internet-based criminality and cybercrime. In particular, VCs are used in activity involving illicit online marketplaces and in cases of hacking and cyber theft. But cybercrime, while increasingly common, is still a relatively new and evolving form of crime. The potential for VCs to abet cybercrime is likely to evolve as cybercrime typologies evolve. The ultimate potential scope and scale of these risks is still unclear.

The situation is far from straightforward. Governments are likely to face a period of trial and error in developing appropriate policy responses. The private sector faces challenges too. Both the VC industry and the established financial sector are working to understand their role in this rapidly evolving landscape.

19. Andy Greenberg, 'Prosecutors Trace $13.4 Million in Bitcoins from the Silk Road to Ulbricht's Laptop', *Wired*, 29 January 2015.
20. Vigna and Casey, *Cryptocurrency: The Future of Money?*, p. 83.
21. Robert McMillan, 'The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster', *Wired*, 3 March 2014.

Yet the story is not just about challenges. VCs offer opportunities and, if managed correctly, stakeholders can develop important new technologies that could improve global financial services.

Expert opinion varies significantly on the likely future of VCs. Some advocates of VCs still believe in the cypherpunk vision of a world where cryptocurrencies will eventually supplant government-issued money. Many in the VC industry are more tempered: they remain staunch advocates of VCs as a financial innovation, but see a variety of potential outcomes. Some see it as unlikely that any altcoins will have the success of Bitcoin; some see it as likely that as-yet-uncreated cryptocurrencies could surpass Bitcoin. Others see Bitcoin as having a clear advantage as a first mover that cornered the market and will continue to grow and dominate as technical enhancements make the Bitcoin network more efficient and scalable.[22]

Where greater agreement has emerged, it is around the general view that VCs offer a crucial experiment in new payment systems, and that certain related innovations – and in particular DLT – have applications well beyond VCs. Whatever their fate, VCs are rapidly challenging notions about how finance, society and technology interact.

This paper aims to contribute to the discussion about VCs and financial crime by exploring stakeholder responses. It considers the literature on the topic, including academic papers, press reporting and white papers from international institutions, government and industry. The author also draws on discussions held between October 2016 and February 2017 with more than a dozen experts in the field. This includes individuals with current or previous experience in the VC industry, law enforcement agencies, regulatory bodies, academia and the banking sector.

This paper aims to provide a non-expert audience with an introduction to VCs and related financial crime issues, while also offering meaningful considerations for expert stakeholders. It offers descriptions of key technical matters related to VCs (where necessary for context and understanding), but does not aim to be exhaustive. Chapter I provides an overview of key financial crime risks related to VCs. It does not consider every potential risk that might emerge, but it discusses some of the more widely debated and examines their implications. A key challenge is the limited amount of concrete quantitative data on financial crime and VCs. Official government reporting on VCs and financial crime is typically anecdotal rather than data-driven. This reflects the newness of VCs. Industry produced estimates of the extent of financial crime activity using VCs are helpful, but discrepancies exist in those figures. Still, sufficient research and reporting exists on the topic to enable informed qualitative assessments.

Another challenge is that regulatory and law enforcement approaches are in their nascent phases. Any examination of their effectiveness must rely on early anecdotal evidence and speculation about possible future impact.

Chapters II–IV consider the implications of these risks for stakeholders in the public sector, the VC industry and the established financial sector. Each chapter sets out targeted recommendations for those stakeholders.

22. Author's discussions with industry experts, October–November 2016.

This paper focuses on the implications of VCs for financial crime-related regulation and policymaking. It does not consider in depth the range of related consumer protection, tax and other issues, but acknowledges these in brief where relevant.

I. Understanding the Financial Crime Risks

VCS HAVE NUMEROUS legitimate applications but also pose a number of financial crime risks. This chapter will describe the most significant of these: anonymity/pseudonymity; rapid international transaction settlement; and decentralisation and contained environments. It will then examine how these risks manifest themselves in the following types of activity: money laundering; terrorist financing; fraud; and cybercrime.

Anonymity/Pseudonymity

Privacy has always been a central aim of VC developers. VCs, however, are not uniformly completely anonymous; rather, they feature varying degrees of anonymity. Bitcoin is 'pseudonymous': users are identifiable throughout the network by their alphanumeric keys. Users can choose to use a single public key for all transactions, but they may also create a new public key for each individual transaction they undertake; indeed, creating unique public addresses for each Bitcoin transaction is common practice as a way of enhancing privacy on the public blockchain.

However, this degree of pseudonymity comes in direct confrontation with the Know Your Customer (KYC) principles at the heart of the global AML/CTF regime. Using KYC, banks and other gatekeepers to the financial system collect information to identify their customers and then verify that information using a customer's passport or other documents. With Bitcoin, one can merely access the network and create a potentially infinite number of pseudonymous 'identities' when transacting with other users.

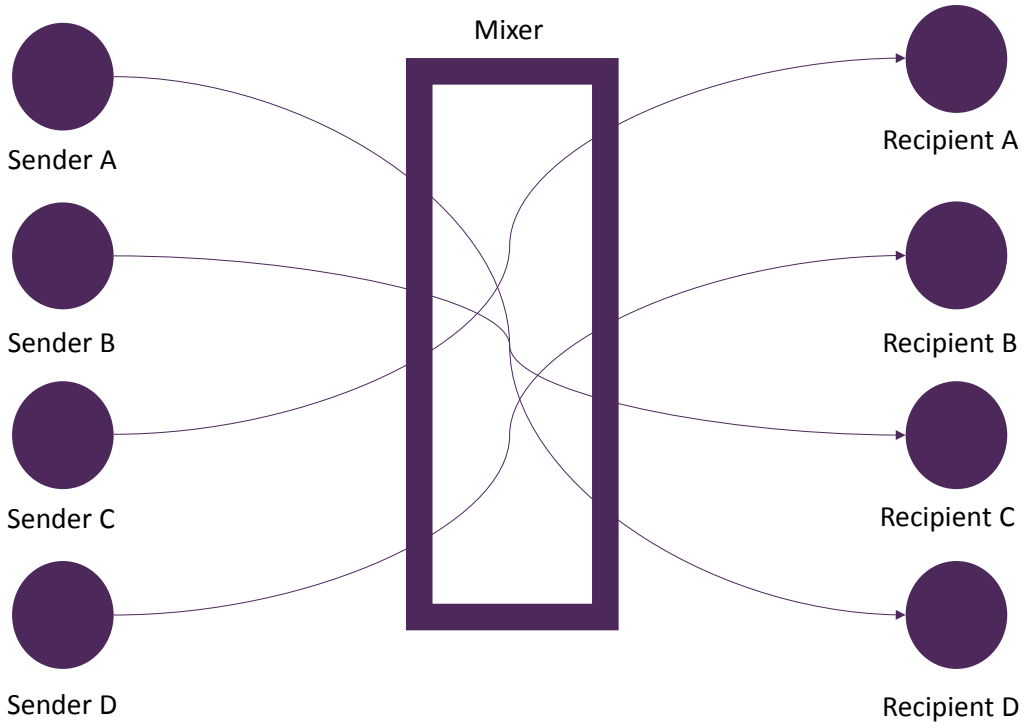
Although pseudonymity seems an obvious boon to criminals, the public nature of the blockchain acts as a mitigant by offering a complete transaction trail. As Malte Möser, a researcher in cryptocurrencies, has noted, 'AML in Bitcoin has to deal with imperfect knowledge of identities, but may exploit perfect knowledge of all transactions'.[1] Consequently, if law enforcement agencies manage to connect an individual to particular Bitcoin wallet addresses, they can have a complete view into that individual's transactional activity. Bitcoin therefore presents a flawed medium for illicit behaviour. As Chapter III of this paper highlights, the private sector has developed a number of tools to detect illicit activity across the Bitcoin blockchain.

The blockchain, however, is not a foolproof crime-fighting tool. A number of solutions exist to permit more genuine anonymity. Mixing services (also known as 'tumblers') enable Bitcoin users to cover their tracks. Not all transactions that use mixers are illicit, but mixers provide an attractive tool for criminals. Mixers aggregate transactions from numerous users and obscure

1. Malte Möser et al., 'An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem,' eCrime Researchers Summit (2013), pp. 1–2.

the actual trail of activity. Figure 1 provides a simple illustration of the concept behind a Bitcoin mixer. Each sender wishes to transfer Bitcoin to a respective recipient wallet (for example, Sender A is transfering Bitcoin to Recipient A). The mixer redistributes the funds among wallets so that it is unclear which bitcoins came from which wallet.

Figure 1: Illustration of the Concept Behind a Bitcoin Mixer



However, mixing activity suffers from limitations: while the precise trail of individual transactions is obscured, the fact that mixing activity has occurred is detectable; efforts to place very large transactions through mixers therefore can signal potentially suspicious activity.[2] Mixers vary in quality as anonymising tools depending on a variety of technical factors, and Kathryn Haun, a US Department of Justice prosecutor, has suggested that US law enforcement agencies have had success in de-anonymising transactions from less effective mixing services.[3] Legitimate users also face a risk of having tainted coins – or bitcoins from an illicit source – sent to their wallet from a mixing service. Chainalysis, a firm that provides blockchain intelligence services, estimated that during the first half of 2016, approximately 160,000 (or 2%) of more than 6 million bitcoin sent worldwide involved mixing.[4] Coinfirm, a London-based consultancy that devises blockchain AML solutions, estimates that up to 10% of the daily value of Bitcoin transactions could involve

2. John Bohannon, 'Why Criminals Can't Hide Behind Bitcoin', *Science*, 9 March 2016.
3. Laura Shin, 'Federal Prosecutor Kathryn Haun On How Criminals Use Bitcoin – and How She Catches Them', *Forbes: Personal Finance*, 1 November 2016.
4. Nathaniel Popper, 'How China Took Center Stage in Bitcoin's Civil War', *New York Times*, 29 June 2016.

mixing.[5] Whatever the exact figures, many Bitcoin users remain septical of mixers, owing in part to their sometimes unreliability and insecurity.

A number of altcoins feature significantly greater anonymity than Bitcoin. These cryptocurrencies include mixing activity or other anonymising features as part of their protocol, rather than an add-on feature. Monero, for example, is a cryptocurrency launched in 2014 that features an opaque blockchain, obscuring the source and destination of a transaction. Monero transactions are not publicly transparent; rather, transaction details are only visible to those with access to a private key, which is individual transaction specific.[6] Another innovative altcoin is Zcash, which launched in 2016, and allows users to choose whether to have transaction details recorded publicly on its blockchain or remain fully encrypted.[7]

Experts debate the viability of these and other altcoins as more than a cyber-enthusiast's tool. Bitcoin, with its financial footprint in the blockchain, remains by far the most widely used. Increasingly, however, cryptocurrency developers are exploring how to balance the need for accountability and legitimacy with a desire for greater privacy than the Bitcoin blockchain affords. As James Smith, Chief Executive of blockchain forensics firm Elliptic observes, 'It is naïve to think we'll move to a world where transactions are completely opaque … but it is realistic to think that we will move to a world of selective transparency.'[8] The ability of cryptocurrencies to integrate and balance concepts of transparency and enhanced privacy in their design will have consequences for regulatory attempts to apply traditional AML/CTF principles.

Rapid International Transaction Settlement

A key innovation of VCs is near real-time transaction settlement at a lower cost than other well-established methods.[9] Nakamoto's innovations enable users to transfer their bitcoins relatively rapidly across the world. This offers hope that new payment methods such as VCs can provide cost-efficient micro-payments (or small online transactions) as well as remittances to underdeveloped countries (Box 1). However, this ability to transact quickly poses risks.

Increasingly, money laundering is occurring on an industrial scale. The UN estimates that total annual illicit financial flows globally exceed more than $2 trillion annually.[10] A single organised criminal network may engage in cross-border financial crime activity in the billions. Terrorist organisations operate globally and use international financial networks. Law enforcement

5. *Coinfirm Blog*, 'What Are Bitcoin Mixers/Tumblers and How Often Are They Being Used?', 7 November 2016.
6. Jordan Pearson, 'Meet Monero, the Currency Dark Net Dealers Hope is More Anonymous than Bitcoin', *Motherboard*, 23 August 2016.
7. Zooko Wilcox and Peter Van Valkenburgh, 'What is Zcash?', *Coin Center*, 8 December 2016.
8. Andrew Quentson, 'Bitcoin is Too Transparent, Says Blockchain Surveillance Firm Executive', *Cryptocoin News*, 14 November 2016.
9. Jason Voss, 'Bitcoin is More Important than You Think', CFA Institute, 29 April 2015.
10. UN Office on Drugs and Crime, 'Money Laundering and Globalization', <https://www.unodc.org/unodc/en/money-laundering/globalization.html>, accessed 8 December 2016.

Box 1: VCs and Financial Inclusion.

One potential application of VCs and related technology relates to financial inclusion – or the expansion of financial services to places where they are presently limited or unavailable. Banks and established transfer agencies, such as Western Union, require a significant legacy infrastructure that involves numerous middlemen and high fees, posing a challenge for underdeveloped countries. Decentralised, electronic payment platforms that are secure, cost-effective and efficient in their delivery offer a potential alternative. As Jerry Brito and Andrea Castillo have noted 'as an open-system payment service, Bitcoin can provide people in developing countries with inexpensive access to financial services on a global scale'.[1]

Mobile payment systems have emerged over the past decade in countries where the number of individuals who own phones outnumbers those with bank accounts.[2] As much as 25% of Kenya's GDP flows utilises M-Pesa, a mobile payments system developed in 2007 by the country's largest telecoms provider, Safaricom.[3] VCs are now part of the equation with the emergence of BitPesa, a payment service that facilitates bitcoin-based currency exchange in Kenya, Uganda, Tanzania and Nigeria.[4] Bitcoin also features increasingly in remittances between individuals across East Asia, in particular in countries such as the Philippines.[5]

Just how large a role Bitcoin or other VCs could play in financial inclusion is unclear. Mobile payment systems are still in their early phase of development. In Africa, cash comprises more than 90% of retail transactions.[6] Bitcoin still has a relatively small user community in Africa, and it is not a panacea to the complex crisis of poverty,[7] but decentralised computing could eventually have a significant role in facilitating low-cost global transactions. The IMF notes that DLT-based payment systems could facilitate financial inclusion in fiat currency, which may offer a more promising solution than VCs.[8] A number of governments, such ask the UK, Canada and China, are looking to cryptocurrency innovations to explore how to create digitised versions of fiat currency. (https://www.ft.com/content/f15d3ab6-750d-11e6-bf48-b372cdb1043a).

---

1. Jerry Brito and Andrea Castillo, 'Bitcoin: A Primer for Policymakers', Mercatus Center, George Mason University, 2013, p. 14.
2. Vigna and Casey, *Cryptocurrency: The Future of Money?*, p. 211.
3. *Ibid*.
4. See, BitPesa, 'Move with Africa: Do Business Across Africa with Easy FX and B2B Payments', <https://www.bitpesa.co/>, accessed 6 February 2017.
5. Luke Parker, 'Bitcoin Remittances "20 Percent" of South Korea–Philippines Corridor', *Brave NewCoin*, 14 September 2016.
6. Alex Lielacher, 'Cash Still Trumps Mobile Payments and Bitcoin in Africa', *Bitcoin Magazine*, 7 December 2016.
7. J P Lawrence, 'The Western Myth of Bitcoin in Kenya', *Motherboard*, 4 January 2016.
8. Dong He et al., 'Virtual Currencies and Beyond: Initial Considerations', IMF Staff Discussion Note, SDN/16/03, p. 19.

agencies worry that VCs could therefore present an attractive opportunity for increasingly globalised criminal and terrorist groups requiring borderless financial channels.

From a technical perspective, Bitcoin is still a maturing system and continued efforts are being channelled into making its core software more efficient. It is not yet able to facilitate genuinely cost-free, instantaneous settlement on the colossal scale that cryptocurrency enthusiasts envision. However, further blockchain innovations offer the prospect of ever-more rapid and cost-efficient payment settlement across borders.[11]

Decentralisation and Contained Environments

Because of the level of attention Bitcoin has received from law enforcement agencies, it is important to consider the specific risks decentralised cryptocurrencies pose.

Miners, exchanges, wallet providers, payment processors, ATM providers and other actors play a vital role in enabling the Bitcoin network to function. However, it is still a decentralised network with no central administrator and runs on an open source software. Whom to hold accountable in cryptocurrency networks is not always clear. As the Financial Action Task Force (FATF) – the global AML/CTF standard-setting body – has noted, '[l]aw enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes … [C]ustomer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them'.[12]

To date, most countries have focused on regulating VC exchanges at the points where users 'cash in' or 'cash out' of VC networks with government-backed fiat currency. FATF endorses the view that the existing AML/CTF regime can be most effective at the point where VCs come into contact with 'real' money and the formal financial system. Placing VC exchanges under AML/CTF regulation enables exchanges to act as a gatekeeper to the fiat money world and to identify illicit actors who may be transferring funds between legal tender and VCs. This also enables law enforcement agencies to identify a clear point of contact for obtaining information on activity occurring on the periphery of the VC ecosystem.

However, this approach does not solve the problem of opacity *within* VC ecosystems. Financial crime risk management experts Joseph Mari, Peter Warrack and Leonardo Real have described this as a problem of interactive versus contained environments.[13] In the former, VC users connect with the established financial system – for example, they convert their bitcoin to pounds sterling on an exchange, have those pounds sent to their bank, and subsequently withdraw their pounds from the bank in cash. While compliance staff at a bank would not see the full transaction trail

11. David S Evans, 'Digital Currency Deep Dive: Is Bitcoin Cheaper and More Efficient than Traditional Payments?', *PYMNTS.com*, 20 June 2014.
12. FATF, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', June 2014, pp. 9–10.
13. Joseph Mari et al., 'When Two Worlds Collide', *ACAMS Today*, September–November 2016, pp. 26–29.

involving VCs, if they are aware that their customers use VCs they can act to mitigate related risks (for example, by conducting enhanced monitoring of customer account activity).[14]

In contained environments, established regulated firms have no role or insight. According to Mari and Warrack, contained environments are those where 'all transactions occur outside the traditional banking system and are only visible within a given blockchain'.[15]

At present, the size of contained environments is likely relatively small. The bulk of Bitcoin transactions still pass through exchanges for conversion into fiat currency.[16] With time, however, contained environments among decentralised VCs could grow, both in absolute scale and relative to interactive environments.

One concern some security experts express is that terrorists or non-state actors might create their own decentralised and highly anonymised VCs, or could do so in coordination with a state sponsor. A study by the RAND Corporation concluded that creating a viable VC is technologically beyond the reach of terrorist groups and other illicit actors at present, but could become feasible if VCs proliferate in their general use.[17] For now, illicit actors using established VCs is more likely.

The prospect of growth in contained VC environments raises a number of critical questions: how should the law treat participants in a contained VC ecosystem? Are traditional AML/CTF approaches relevant? Should governments attempt to regulate those contained environments at all? Chapter II of this paper will examine how governments are responding to these and related questions.

Money Laundering

The Silk Road case drew public attention to the potential of VCs to facilitate crime. VCs have a rapidly growing role among cybercriminals, but among more traditional criminal operatives that engage in large-scale money laundering – such as large drug cartels and human-trafficking networks – the picture is more mixed.

Given the limited scale of contained VC environments, money laundering involving VCs is likely to occur through two generic methods. First, criminals could place dirty fiat currency into a bank or other financial institutions, convert those funds to VCs using a VC exchange, and then engage in a variety of VC-based transfers or purchases to obscure the funds' criminal origin. Second, criminals could sell illegal goods or services for VCs, eventually convert those to fiat currency, and subsequently fund transactions and purchases designed to conceal their illicit source.

14. *Ibid.*
15. *Ibid.*
16. Popper, 'How China Took Center Stage in Bitcoin's Civil War'.
17. Joshua Baron et al., *National Security Implications of Virtual Currency: Estimating the Potential for Non-State Actor Deployment* (Santa Monica: RAND Corporation, 2015).

Established criminal networks have demonstrated an interest in Bitcoin, but they are not yet using it in significant volumes for money-laundering activity. As the UK National Crime Agency (NCA) noted in September 2016, '[VCs] have yet to be adopted to any large degree by money launderers'.[18] However, the NCA did suggest that 'potential remains for this area to develop into a major risk'.[19] In early 2017, Dutch prosecutors indicated that they were pursuing a case against a major money-laundering organisation utilising Bitcoin. However, at the time of publication, details of that case had not been publicly released and a trial is not expected to commence until the end of 2017.[20]

Cases of money laundering using VCs certainly exist. In some cases, operators of centralised, convertable VC schemes have been complicit. Unlike Bitcoin and other cryptocurrencies, centralised VC schemes are issued and overseen by a network administrator that can control network activity. Most prominent is the case of Liberty Reserve, which US authorities shut down in 2013. Liberty Reserve was a Costa Rica-based online payment system that issued its own VC and knowingly facilitated money-laundering activity among criminals. According to US authorities, Liberty Reserve processed '78 million transactions with a combined value of $8bn (£5.5bn) – many of which were related to hiding the proceeds of credit card theft, identity fraud, hack attacks and Ponzi … schemes'.[21] The US government arrested Liberty Reserve's founders and administrators for their involvement in facilitating financial crime.

Among decentralised VCs, such as Bitcoin and other cryptocurrencies, it is with dark web activity that money-laundering risks have emerged. The dark web is accessible only through encrypted networks such as Tor. Illicit online marketplaces – whose existence predates Bitcoin – are seen as democratising criminal activity: they lower barriers to entry by enabling nearly any individual with access to a computer, such as the Silk Road's founder Ross Ulbricht, to facilitate illegal transactions without the associated costs of traditional criminal enterprises. Silk Road was only one of a rapidly growing number of criminal sites on the dark web. One study estimates that when it was operational, Silk Road-related business accounted for as much as 4–9% of all Bitcoin exchange activity.[22]

Chainalysis's figures from the first half of 2016 suggest that the dark market activity is now a smaller portion of overall Bitcoin flows relative to speculative trading than it was when Silk Road operated.[23] Advocates hope that, with time, Bitcoin will continue to gain legitimacy among the

18. National Crime Agency (NCA), 'National Strategic Assessment of Serious and Organised Crime 2016', 9 September 2016, p. 29.
19. *Ibid.*
20. *DutchNews.nl,* 'Dutch Public Prosecutor Cracks Down on Bitcoin Laundering', 3 January 2017.
21. *BBC News*, 'Liberty Reserve Digital Cash Chief Jailed for 20 Years', 9 May 2016. A Ponzi scheme refers to a form of investment fraud in which early investors steal later investors' funds with the promise of securing high returns.
22. Nicolas Christin, 'Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace', Carnegie Mellon University CyLab, 28 November 2012, pp. 19–20.
23. Popper, 'How China Took Center Stage in Bitcoin's Civil War'.

general public and will feature with less frequency in the dark web. However, as the NCA has noted, 'Bitcoin remains the virtual currency of choice' for dark web trading.[24]

As traditional organised crime groups improve their technological capabilities and expand their presence in the dark web, the potential for their expanded use of Bitcoin could grow concurrently. In its March 2017 Serious and Organised Crime Threat Assessment (SOCTA), Europol notes that, 'For almost all types of organised crime, criminals are deploying and adapting to technology with ever greater skill and to ever greater effect,' with organised crime moving increasingly to the dark web.[25] Recent reporting suggests that Italy's Camorra crime gang has sold counterfeit British passports on the dark web, offering the documents for Bitcoin.[26] However, it is unclear from the public record just how extensively the Camorra and other similar crime organisations are using Bitcoin.

Other cryptocurrencies have a place in dark markets. In September 2016, the dark market site Alphabay announced it would begin accepting payment in Monero, due to the VC's enhanced anonymity features.[27] One recent report suggests Monero may account for 2% of Alphabay's sales – a figure that could total in the millions of dollars.[28] Europol notes that, '[t]he majority of law enforcement currently has its attention focused on Bitcoin, a fact which is not lost on the criminal community … some smaller criminal communities may be abusing lesser-known cryptocurrencies in order to stay under the radar'.[29] The use of highly anonymised VCs on encrypted dark web platforms raises the prospect that law enforcement may be operating with blind spots.

A number of money-laundering services have emerged in dark markets. Individual launderers provide 'cash-out' services – that is, they will accept illicit-origin cryptocurrency and arrange for the delivery of pounds or other fiat currency.[30] In December 2016, Europol announced it had arrested eight individuals in connection with a scheme to purchase counterfeit euros with Bitcoin on the dark web.[31] Drug dealers appear to be testing these waters. In early 2016, Dutch authorities arrested ten people on suspicion of laundering funds for drug dealers.[32] The launderers allegedly converted bitcoin proceeds from the drug sales into euros, which, according to prosecutors, they then withdrew at ATMs. The US Drug Enforcement Administration indicates

24. NCA, 'National Strategic Assessment of Serious and Organised Crime 2016', p. 7.
25. Europol, *SOCTA 2017: EU Serious and Organised Crime Threat Assessment* (The Hague: European Police Office, 2013), p. 24.
26. Barbie Latza Nadeau, 'ISIS Can Buy U.K. Passports on the Deep Web to Thwart Brexit Security', *The Daily Beast*, 10 February 2017.
27. Yuji Nakamura, 'New Digital Currency Spikes as Drug Dealers Get More Secrecy', *Bloomberg Technology*, 30 August 2016.
28. Andy Greenberg, 'Monero, the Drug Dealer's Cryptocurrency of Choice, Is On Fire,' *Wired*, 25 January 2017.
29. Europol, *IOCTA 2016: Internet Organised Crime Threat Assessment*, p. 44.
30. Joseph Cox, 'Dutch Police Bust Multi-Million Dollar Bitcoin Laundering Ring', *Motherboard*, 20 January 2016.
31. Europol, 'Eight Arrests in Counterfeit Euro Operation Supported by Europol', press release, 8 December 2016.
32. *Ibid*.

it has intelligence reporting that Colombian narcotics traffickers have used Bitcoin in money-laundering schemes, although the extent of this alleged activity is unclear.[33]

Human traffickers are also using cryptocurrency in online marketplaces. This includes accepting Bitcoin on online escort sites that credit card companies have refused to service.[34] However, one study has noted that while human traffickers may be adopting Bitcoin and other new technologies, this 'may not be a major component of the crime in practical terms'.[35]

In the Dutch drug-related case, law enforcement apprehended the alleged money launderers after reportedly linking them to activity on the Bitcoin blockchain.[36] This transparency likely accounts for one reason large traditional criminal networks have not rushed into Bitcoin as a major funding tool and away from traditional funding methods. Usability is another factor. Using VCs requires an adeptness with online transactions and platforms that many established criminal networks may not have acquired yet.[37] Cryptocurrencies, furthermore, while growing in use, are not in sufficient circulation to facilitate business on the scale that major criminal organisations require. And while cryptocurrencies represent a new payment method whose use large criminal enterprises may be keen to test, Europol's 2017 SOCTA notes that, 'Cash remains at the core of the money laundering business'.[38] Most criminals are likely to heavily favour cash and other more traditional financial products for some time.

Terrorist Financing

The rise of Daesh (also known as the Islamic State of Iraq and Syria, or ISIS) has raised law enforcement concerns that global terrorist organisations could use VCs to finance attacks.

Terrorist financing with VCs is best regarded as an emerging and potential risk, rather than a crystalised one. As Europol noted in January 2016, '[d]espite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by [European] law enforcement'.[39]

In the near term, terrorist organisations may find VCs technically and practically difficult to use. Terrorists already have established methods for funding attacks, such as the use of remittance agencies in the Middle East. They likely do not see a pressing need to use VCs. Daesh members

33. US Department of Justice Drug Enforcement Administration, 'National Drug Threat Assessment', 2015, p. 96.
34. Sasha Aslanian, 'For Sex Industry, Bitcoin Steps In Where Credit Cards Fear to Tread', *NPR*, 15 December 2015.
35. Hayley Watson et al., 'Role of Technology in Human Trafficking', TRACE Briefing Paper, October 2015, p. 12.
36. Bohannon, 'Why Criminals Can't Hide Behind Bitcoin'.
37. HM Treasury, *Digital Currencies: Response to the Call for Information* (London: The Stationery Office, March 2015), p. 12.
38. Europol, *SOCTA 2017*, p. 18.
39. Europol, 'Changes in Modus Operandi of Islamic State Terrorist Attacks: Review Held by Experts from Member States and Europol on 29 November and 1 December 2015', 18 January 2016, p. 7.

have often relied on simple funding methods, such as acquiring student loans.[40] Financing terrorist operations requires simple but straightforward and reliable funding; transactions using Bitcoin – which sometimes has dramatic price swings – may prove unattractive beyond occasional, one-off use.

Reporting on terrorist financing using Bitcoin remains limited and largely anecdotal. In August 2015, a US teenager received an eleven-month jail sentence for, among other things, using Twitter to describe how to use Bitcoin to support Daesh.[41] A former US intelligence analyst has identified an instance of low-value Bitcoin fundraising by a media organisation affiliated with a Palestinian group the US has labelled a terrorist organisation.[42] Most recently, in January 2017, the Indonesian government announced its assessment that Bahrun Naim, an Indonesian Daesh operative who is the alleged organiser of a 2016 terrorist attack in Jakarta, had used Bitcoin in transactions with other jihadis. However, the Indonesian government has not released specific details about how this activity occurred and whether it was instrumental to any attacks.[43]

Security experts have expressed concern that terrorists are becoming rapidly more technologically adept;[44] as this trend continues, VCs could become an increasingly viable financing tool for terrorists. Terrorists us VCs to purchase illegal firearms or explosive material on the dark web, as well as travel documents or other items to facilitate operations. VC exchanges also present risks where they remain unregulated in countries with high levels of terrorist financing, such as Pakistan.[45] Experts express concern that blockchain innovations, such as the use of 'smart contracts',[46] could enable terrorist organisations to finance attacks.[47] DLT experts regard smart contracts as one of the more promising blockchain innovations, with the potential to simplify legal agreements and transfer of assets among counterparties involved in complex arrangements. These are self-executing contracts based on a blockchain that enable parties to agree a set of terms and subsequently release payment on the completion of pre-agreed actions. One hypothetical financial crime scenario involves terrorist networks using smart contracts to arrange and fund attacks. Similarly, criminals could use smart contracts to arrange for payment on the completion of any illicit activity, such as the delivery of drugs or carrying out of an assassination.[48]

40. Martin Bentham, 'Call for Action to Stop Islamic State "Funding UK Plots with Student Loans"', *Evening Standard*, 18 August 2015.
41. US Department of Justice, 'Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL', 15-1057, press release, 28 August 2015.
42. Yaya Fanusie, 'The New Frontier in Terror Fundraising: Bitcoin', *Cipher Brief*, 24 August 2016.
43. Pete Rizzo, 'Indonesia's AML Watchdog Links Bitcoin to Islamic State', *CoinDesk*, 9 January 2017.
44. Grant Gross, 'Terrorists are Winning the Digital Arms Race, Experts Say,' *Computerworld*, 17 January 2017.
45. P Carl Mullan, 'Money Laundering and Funding Terror Using Bitcoin and Other Digital Currency Products', *scribd.com*, 12 April 2014, p. 25.
46. Giulio Prisco, 'The Future of Smart Contracts: Positive Social Innovation or Criminal Activity?', *Bitcoin Magazine*, 19 August 2015.
47. Stan Higgins, 'ISIS-Linked Blog: Bitcoin Can Move Terrorist Funds Worldwide', *CoinDesk*, 7 July 2014.
48. Prisco, 'The Future of Smart Contracts: Positive Social Innovation or Criminal Activity?'.

However, for all the concern, there is no concrete indication in the public record that terrorists are using cryptocurrencies as a payment tool with regularity.

Fraud

VCs carry a number of fraud risks. First is the risk of VC users committing fraud. One strength of Bitcoin is the blockchain's immutability – once a transaction is confirmed it cannot be reversed or terminated in the manner that a credit card company or bank can reverse or cancel transactions. However, this exposes users to risks. In VC networks, purchasers are not always protected against failure to deliver goods, or if they receive counterfeit or faulty goods. The anonymous/pseudonymous nature of VCs allows fraudsters to operate under concealed identities, misrepresenting themselves in online marketplaces to carry out fraud.

A second major risk comes directly from VC exchanges and service providers. A number of well-publicised cases exist of Bitcoin exchanges operating as Ponzi schemes.[49] Unregulated Bitcoin exchanges have also simply disappeared, shutting down and stealing their misled customers' deposits.[50] Chainalysis estimates that across the first half of 2016, approximately 140,000 of more than 6 million global Bitcoin sent, or approximately 2%, were related to scams or Ponzi schemes.[51] VCs therefore present important consumer protection issues that demand the attention of industry and governments, and speaks to the benefits of regulation as a means for building trust in VCs among the general public.

One hypothetical risk Bitcoin mining poses is a '51% Attack'. If a single miner, or a group of them, obtained over 50% of the computational power required to mine Bitcoin, they could collude to manipulate the network for their own benefit. This could involve recording fraudulent transactions on the blockchain; or they might refuse to approve legitimate transactions. Experts debate the feasibility of conducting a 51% Attack, and the likely severity were one to occur.[52] The cost of obtaining that degree of computing power is huge, and that acts as a deterrent; and miners already have a financial incentive in the form of bitcoin rewards that would make sabotaging the network possibly self-defeating. As Nakamoto described the manner in the original Bitcoin white paper, an attacker 'ought to find it more profitable to play by the rules … than to undermine the system and the validity of his own wealth'.[53] But the debate reflects concerns about a potential vulnerability of the Bitcoin network and remains an active point of discussion in cryptocurrency communities.

49. US Securities and Exchange Commission, Office of Investor Education and Advocacy, 'Investor Alert: Ponzi Schemes Using Virtual Currencies', SEC Pub. No. 153 (7/13).
50. Kadhim Shubber, '$4.1 Million Goes Missing as Chinese Bitcoin Trading Platform GBL Vanishes', *CoinDesk*, 11 November 2013.
51. Popper, 'How China took Center Stage in Bitcoin's Civil War'.
52. See, for example, Daniel Cawrey, 'Are 51% Attacks a Real Threat to Bitcoin?', *CoinDesk*, 20 June 2014.
53. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', p. 4.

Cybercrime

The most pressing and significant immediate risk that VCs pose relates to their use in cybercrime. Cryptocurrencies have become a favoured tool of hackers and online thieves. Europol noted in its *2016 Internet Organised Crime Threat Assessment* that, 'cryptocurrencies, specifically Bitcoin, remain the currency of choice for much of cybercrime, whether it is used as payment for criminal services or for receiving payments from extortion victims'.[54]

Cybercriminals are increasingly favouring on Bitcoin in 'ransomware' attacks, or malicious programmes that encrypt data on servers, computers or mobile devices, and for which criminals then demand a ransom to decrypt. Ransomware has existed for more than two decades, so is not a new phenomenon; but it is a rapidly growing source of cybercrime. Business that are the targets of ransomware attacks are increasingly making payments to hackers. Cryptocurrencies can help criminals get around the risks of capture that come with having to arrange the delivery of ransom payments by hard cash or through bank accounts.

Hackers have launched attacks recently against hospitals, banks and other retailers, encrypting patient or customer data or other sensitive information and seeking bitcoin ransoms.[55] In a recent case, cybercriminals hacked the electronic key system of an Austrian hotel, locking all of its doors; the hotel owners paid the hackers a bitcoin ransom worth $1,800 to have the doors unlocked.[56] According to a report by the security analysis firm Carbon Black, in 2016 companies made more than $850 million in ransomware payments to hackers, a nearly 40-fold increase from $24 million in 2015 – although it is not clear just how much of this is comprised of cryptocurrency payments.[57] The FBI also alleges that other cryptocurrencies, including Monero, are used in approximately 25% of the ransomware cases it encounters.[58] While cryptocurrecies are certainly not the cause of ransomware, cybercriminals appear to have recently found in them a convenient means for extorting payments from victims.

Cybercriminals also directly attack VC exchanges and wallet providers, as occurred in the mid-2016 hack of the Bitfinex exchange that robbed users of bitcoins worth $72 million.[59] These attacks aim to obtain the unique 'private keys' associated with users' public wallet addresses, and which a user must possess to make a transfer. Consequently, large VC service providers are dedicating increasing effort to cyber defences. A number of practical anti-cyber theft practices exist for users to protect themselves. 'Cold' wallet storage – maintaining VC in a wallet that

54. Europol, *IOCTA 2016*, p. 8.
55. Jamie Doward, 'City Banks Plan to Hoard Bitcoins to Help Them Pay Cyber Ransoms', *The Guardian*, 22 October 2016.
56. Dan Bilefsky, 'Hackers Use New Tactic at Austrian Hotel: Locking the Doors', *New York Times*, 30 January 2017.
57. Carbon Black, 'Carbon Black Threat Report: Non-Malware Attacks and Ransomware Take Center Stage in 2016', December 2016, p. 8.
58. Michael del Castillo, 'To Catch a Ransomer: How the FBI Chases Crime on the Blockchain', *CoinDesk*, 1 February 2017.
59. Clare Baldwin, '"Grumpy Hold-Outs" Could Sink Bitfinex Recovery Plan after Bitcoin Theft', *Reuters*, 15 August 2016.

remains offline when it is not in use – is one such method; the use of multi-signature ('multi-sig') wallets, which require more than one private key to initiate a transaction, is another.[60] As the most prominent cryptocurrency, Bitcoin exchanges and wallets will likely be targets of cybercriminals for some time.

VCs present a varied and rapidly changing financial crime landscape. Although they still do not come close to the scale of illicit financial flows using cash, credit cards or other traditional methods, VCs frequently feature in the growing online criminal trade – offering a possible hint of the future direction of financial crime.

However, it is still too soon to say just how VCs might evolve in criminal typologies over the longer term. As the next chapter will discuss, a regulatory approach that assumes VCs are primarily problem of criminality is likely to face significant challenges.

60. Alyssa Hertig, 'What the Bitfinex Hack Means for Bitcoin Multi-Sig Security', *CoinDesk*, 5 August 2016.

II. The Public Sector

This chapter offers observations regarding the public sector's responses to VCs and sets out recommendations for public sector stakeholders.

Observation 1: Regulation

Regulation is in a transitory phase and will likely require adjustment and re-evaluation.

Regulating a new and rapidly evolving financial technology puts governments in a bind: if they do too little too slowly, they may find themselves unable to manage risk; if they do too much too soon, they could stifle innovation and embed an ineffective regulatory framework.

Consistent with FATF's guidance, a number of countries have applied their AML/CTF regulation to VC exchanges, focusing on the points at which VCs interact with the fiat currency world. Regulation of VC exchanges helps to bring oversight to a clearly defined segment of the VC services industry without necessarily being overly restrictive, and the VC industry has generally accepted this approach. Countries that have, or have indicated their intention to, regulate VC exchanges include Australia, Canada, China, Hong Kong, Japan, South Korea, Switzerland, the UK and the US.

The EU's inclusion of VC exchanges in its 5th Money Laundering Directive (MLD) is therefore in line with the emerging practices of other advanced economies. Indeed, some observers have suggested that the EU and the UK have been too slow to regulate exchanges, ultimately hindering the industry. Eitan Jankelewitz, a technology lawyer, has written:

> The lack of regulation in the UK has caused more problems than opportunities for bitcoin businesses. Unable to be sure of what regulation is on the horizon and keen to avoid future liability, bitcoin businesses often find themselves taking more regulatory measures than regulated businesses … With the regulatory picture unclear, banks consider it too risky to offer bitcoin businesses a bank account.[1]

Regulation of exchanges therefore represents a meaningful and measured response to enabling accountability at the periphery of decentralised VC networks, as well as providing the general public with confidence in the soundness of the VC industry. However, the EU measures go a step further than many jurisdictions by also explicitly requiring the regulation of custodial wallet providers, which – at the time of this paper's publication – the EU Parliament recommended defining as: 'an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to holding, store and transfer virtual currencies.'[2] This also marks an

1. Eitan Jankelewitz, 'Bitcoin Regulation in the UK', *CoinDesk*, 16 February 2014.
2. European Parliament, 'On the 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

attempt to enable partial oversight of activity that occurs within the contained environments discussed earlier.

This approach remains largely untested globally, so the EU's measures will offer a case study in regulation of wallet providers.[3] US federal regulatory actions focusing on VC exchanges, centralised VC administrators and payment processors have made no specific mention of wallet providers – though certain wallet provider models may fall within the scope of US regulation.[4] The Philippines, which issued regulations on VC exchanges in January 2017, requires that exchanges that provide wallet services should have effective cybersecurity programmes in place, but does not otherwise regulate non-exchange-based wallet services.[5]

Some observers have questioned the appropriateness of the EU's proposed approach of regulating all commercial entities that offer a custodial wallet service and hold users' keys but are not themselves responsible for the exchange of VCs to fiat currencies.[6] Wallet providers operate with sometimes complex models that do not always fit comfortably into traditional models of financial activity. As Peter Van Valkenburgh has noted, custodial wallet services may:

> appear similar to deposit taking. However, this is not generally an accurate characterization … The digital currency is simply stored in the customer's name in a secure facility usually on-premises, rather like a digital safety deposit box … safekeeping digital currency credentials is something new that falls between traditional custodial key escrow services and fiduciary trust services'.[7]

This could make it a challenge technically and legally to determine which types of wallet providers to regulate. Some VC industry participants suggest that the scope of the EU's requirements on wallet providers is unclear and creates confusion about which types of wallet services would actually be regulated. One concern the industry has expressed is that the measures as drafted could cover multi-sig wallet providers, even though those providers often hold only one of several user keys and may not ultimately exercise control over the users' VCs.[8] An April 2016 UK government report suggested that regulating wallet providers 'would not deliver any benefits

for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC (COM(2016)0450 – C8-0265/2016 – 2016/0208(COD))', A8-0056/2017, 9 March 2017.

3. Peak Suisse, 'Blockchain and the Environment for KYC/AML', <http://peak-suisse.com/blockchain-kyc-aml-europe/>, accessed 9 December 2016.
4. Douglas King, 'Banking Bitcoin-Related Businesses: A Primer for Managing BSA/AML Risks', Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, February 2016.
5. Bankgo Sentral Ng Pilipinas, Circular No. 944, 'Guidance for Virtual Currency Exchanges', January 2017, <http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c944.pdf>, accessed 26 February 2017.
6. Aaron van Wirdum, 'Dutch Bitcoin Companies Start Initiative to Adjust Proposed European Union AML-Directive', *Bitcoin Magazine,* 14 July 2016.
7. Peter Van Valkenburgh, 'Comments to the Office of the Comptroller of the Currency on Exploring Special Purpose National Bank Charters for Fintech Companies', *Coin Center*, 13 January 2016, pp. 3, 8.
8. Jerry Brito, 'Maybe the EU's Proposed AML Rules are Not So Clear After All', *Coin Center*, 15 July, 2016, <https://coincenter.org/link/maybe-the-eu-s-proposed-new-aml-rules-are-not-so-clear-after-all>, accessed 26 February 2017.

in terms of mitigating money laundering and terrorist finance risk, and would place significant burdens on firms in this innovative and embryonic sector.'[9]

However, the European Commission contends that custodial wallets effectively act as a bank account within a VC network, and that those holding users' keys should be regulated to reliably connect real identities to their activity.[10] Proponents of regulating wallet providers also point out that many large wallet providers already implemented AML/CTF policies even before coming under regulation.[11] The EU experience in wallet provider regulation will likely determine whether and how other countries follow. As of early 2017, the Australian government was consulting with industry on its proposal to regulate wallet providers.[12]

As of the time of this paper's publication, it is unclear just how far the extent of the EU's requirements will extend. In March 2017, the EU Parliament issued a report which proposed amendments to extend requirements for AML/CTF regulation even beyond VC exchanges and custodial wallet providers. The suggested changes would require regulation of 'issuers, administrators, intermediaries and distributors of virtual currencies'.[13] Its ultimate potential impact on the VC industry is unclear, and much would rest on important matters of practical implementation, such as the definition of an 'intermediary'. Whatever approach the EU finally settles on, it should make the intended scope of its measures clear to avoid confusion among member state regulators and the VC industry.

Thus, despite an emerging consensus on regulating VC exchanges as a baseline measure, the global regulatory landscape still contains disagreements about approaches and aims. Some countries have yet to decide whether to regulate VC exchanges and other service providers and are still determining their approach. Other countries, such as Iceland, Bangladesh and Ecuador, ban all dealings in VCs from within their jurisdiction. Legislative frameworks are also often unclear in their scope. For example, in a number of countries the status of VC ATMs under AML/CTF regulation is uncertain.[14]

Some variation in the global regulatory landscape is perhaps inevitable at this early stage. Banning VCs outright, however, is generally futile, unmerited and counterproductive. As

9. Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (London: The Stationery Office, 2016), p. 19.
10. European Commission, 'Impact Assessment: Accompanying the Document. Proposal for a Directive of the European Parliament and the Council 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 Directive 2009/101/EC', SWD (2016) 223, 5 July 2016.
11. *Ibid.*
12. Australian Government, Attorney-General's Department, 'Regulating Digital Currencies under Australia's AML/CTF Regime – Consultation Paper', December 2016, p. 10.
13. European Parliament, 'On the 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 Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC (COM(2016)0450 – C8-0265/2016 – 2016/0208(COD))', p. 118.
14. The Commonwealth, 'Working Group on Virtual Currencies: Working Group Report', October 2015, p. 17.

a 2015 UK government consultation on VCs suggested, banning them could 'drive market participants underground, reduce visibility of transactions and encourage the appropriation of the technology by criminals instead of legitimate users'.[15] Heavy-handed responses that seek to ban VCs, or prohibit certain applications of their use, fail to grasp the nature of the technology. Ultimately, preventing all dealings in online, decentralised networks is impractical. Countries such as Russia and Thailand that announced intended bans on VCs have in practice allowed the trade to operate and are revisiting their approach.[16]

At a January 2017 conference for law enforcement sponsored by Europol, Interpol and the Basel Institute on Governance, one recommendation put forth was for countries to take action against tumblers and mixers, and suggested that '[t]he existence of such companies should not continue to be tolerated.'[17] In its March 2017 amendments to the 5th MLD, the European Parliament suggested amending the text of the 5th MLD to read that, 'virtual currencies cannot be anonymous',[18] suggesting a possible intolerance for mixing or other similar technology.

In practice, a formal attempt to ban mixing would be highly problematic. First, one consequence might merely be to drive mixing activity further underground without disruption of illicit use. Sophisticated cybercriminals would still be likely to find ways to use anonymising tools. Second, it dismisses without discussion concerns about user privacy. Because the Bitcoin blockchain is public, some legitimate Bitcoin users see mixers as an important tool for protecting their personal data. The BITCRIME Project, a recent study commissioned by the German and Austrian governments, notes that the use of anonymisation techniques can involve 'justified data protection reasons', and represents 'the exercise of a fundamental right to informational self-determination in view of a transaction history which is public in principle'.[19]

Altcoins such as Monero and Zcash are founded on similar principles to mixers; namely, that if cryptocurrencies are going to be viable, having data made fully available on public ledgers in the manner of Bitcoin is problematic. These highly anonymised cryptocurrencies thus aim to choose the level of third-party visibility over their transactions – much in the manner one might choose to conduct some transactions via credit card, while conducting others in cash. While these highly anonymised cryptocurrencies could appeal to criminals, it is important also to ask whether the threat is so great that it requires restricting or otherwise deligitimising cryptocurrencies at the expense of giving law-abiding individuals discretion and privacy in their

15. HM Treasury, *Digital Currencies: Response to the Call for Information* (London: The Stationery Office, 2015), p. 13.
16. Evander Smart, 'Top 10 Countries Where Bitcoin is Banned', *Cyrptocoins News*, 27 May 2015.
17. Basel Institute on Governance, 'Global Conference on Countering Money Laundering and Digital Currencies', <https://www.baselgovernance.org/news/global-conference-countering-money-laundering-and-digital-currencies>, accessed 14 February 2017.
18. European Parliament, 'On the 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 Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC (COM(2016)0450 – C8-0265/2016 – 2016/0208(COD))', p. 102.
19. Rainer Böhme et al., 'Bitcoin and Alt-Coin Crime Prevention: A Recommendation for the Regulation of Virtual Currencies', January 2017, p. 32.

financial affairs. What's more, it is impractical to assume this open source technology can be put back in its box. Law enforcement agencies may very well have to adjust to a world where 'selective transparency' exists.

Preferable to banning this type of technology would be for governments to develop publicly available money-laundering typologies and case studies describing their use in illicit activity so that the private sector can make risk-based determinations about whether certain activity requires reporting to law enforcement agencies. This would make clear that certain types of activity represent higher-risk activity, but would also protect the right of legitimate users to privacy.

Another recent development in the EU is discussion about whether eventually to limit the permissible value of VC transactions. In January 2017, the European Commission set out an impact assessment to consider the consequences of enacting upper limits on cash transaction values. Citing the use of cash in terrorist activity, the assessment argues that restricting the values of permissible cash transactions would rob terrorists, tax fraudsters and other criminals of an anonymous payment method; the report also suggests that 'an option could be to extend the restrictions … to all payments ensuring anonymity (cryptocurrencies, payments in kind, etc.)'.[20]

This would mark a drastic step, and an ultimately deterministic one: if enacted in the near future, it would represent a clear signal from the public sector that VCs should be limited in their scope and use. As a risk mitigation measure, it would represent a premature action in that, as noted earlier, knowledge about the use of VCs in terrorism and other crimes is still only developing and extended restrictions could possibly stifle VC innovation at an early stage in its history.

One possible retort to this argument is that cryptocurrencies enable flourishing of new types of crime, such as dark web activity and increased ransomware attacks, and restricting their use could be critical to curtailing those crimes. This counterargument suffers from two major weaknesses. First, the activities with which cryptocurrencies are frequently associated do not represent entirely new forms of crime, but rather represent the transition of long-established crimes to new environments; merely banning cryptocurrencies will not solve the complex problems that underlie data protection issues relevant to ransomware attacks. Second, law enforcement agencies are still in the early stages of adapting to ransomware and other online crimes. An FBI special agent recently described publicly that US law enforcement agencies are able to track the activity of ransomware attackers using a combination of analytical tools designed for blockchain analysis, as well as more traditional investigative methods.[21] Rather than rushing to restrict the use of VCs, practical law enforcement efforts to adapt to new challenges should be given time.

It will be important for governments to develop coherent responses to these complex issues. With time, a more harmonised international framework for VCs would be preferable to the

20. European Commission, 'Proposal for an EU Initiative on Restrictions on Payments in Cash', 23 January 2017, p 5.
21. Del Castillo, 'To Catch a Bitcoin Ransomer: How the FBI Chases Crime on the Blockchain'.

current ad hoc and uneven landscape. A borderless, decentralised payment method warrants a response that recognises its global nature. Even countries that regulate VC exchanges vary significantly in terms of the timeliness of their implementation and in the vigorousness of their enforcement. Fragmentation across borders could stifle VC innovation while failing to manage the financial crime risks appropriately. As the European Banking Authority (EBA) has noted, '[g]iven the transnational nature of VCs, it is … important that Member States and competent authorities approach the new AML/CFT regime … consistently across the EU'.[22] While the EU's measures provide for uniform high-level requirements across the bloc, ultimately VC exchanges and wallet providers will have to receive licences in each individual country, a fact some VC advocates suggest could act as a barrier to entry for small start-ups.[23] Variance in the ongoing implementation of AML/CTF measures by member states could prove challenging for VC start-ups to manage as well.

The US offers a cautionary tale in the risks of fragmentation. In addition to having to meet national-level AML/CTF regulations on money transmitters, VC exchanges and administrators in the US face separate licensing requirements across nearly all 50 states. This state-based licensing regime is not unique to the VC industry and indeed impacts other types of financial institutions, such as traditional fiat currency money remitters. However, the VC industry has been particularly vocal in describing the downsides of state-by-state licensure in hindering financial innovation. One Bitcoin advocacy group called state licensing 'a duplicative, laborious, and expensive process that presents a barrier to interstate commerce without much benefit to consumers'.[24] Indeed, the US government is now considering a single national licensing regime for VCs and other fintech (financial technology) innovators.[25]

Firms in the US also face variance in state-by-state AML/CTF requirements. The most significant example is New York State's BitLicense regime, which launched in mid-2015. BitLicense requires VC exchanges, administrators and a range of other service providers to register with state authorities. To obtain a licence, firms must meet a number of stringent requirements related to AML/CTF, cyber security, record-keeping and other measures. State officials have hailed the move as a novel approach, aimed at making New York a welcome and safe environment for VC firms; but the VC industry has criticised it as burdensome and too broad in its application. As of January 2017, only three licences had been granted, with at least 25 applications having been submitted since the BitLicense programme launched; a number of firms in the VC industry have moved operations from New York or abandoned plans to locate there.[26]

22. European Banking Authority, 'Opinion of the European Banking Authority on the EU Commission's Proposal to Bring Virtual Currencies into the Scope of Directive (EU) 2015/849', EBA-Op-2016-07, 11 August 2016, p. 3.
23. Michael Scott, 'EU State-By-State Regulation of Bitcoin, Digital Currencies: What are the Implications?', *Bitcoin Magazine*, 5 December 2016.
24. Brito and Castillo, 'Bitcoin: A Primer for Policymakers', p. 37.
25. Peter Van Valkenburgh, 'The OCC Has Decided to Pursue the Federal Fintech Charter For Which We Have Been Advocating', *Coin Center*, 2 December 2016.
26. Suzanne Barlyn, 'New York's Bitcoin Hub Dreams Fade with Licensing Backlog', *Reuters*, 31 October 2016; Joseph Young, 'Coinbase Obtains BitLicense, Only Exchange in New York to Comply', *BTCManager.com*, 19 January 2017; New York State Department of Financial Services, 'NYDFS

BitLicense is an example of an attempt to create a customised regime before regulators fully understood the implications of their proposed approach. As the UK's consultation suggests, it may be 'premature to draw up a bespoke regime given digital currencies are still in a very early stage of development and it is difficult to predict what direction the technology might go in'.[27]

However, the UK consultation also notes the view of some industry participants that, '[in] principle, an ideal solution would be a new regime, designed to address the distinctive nature of [VCs]'.[28] Limited measures underway to regulate VC exchanges represent a prudent attempt to manage risk without strangling industry. With time, however, regulators should consider whether new frameworks and approaches are required, and they should be willing to reexamine traditional assumptions about effective AML/CTF practice as applied to VCs. This does not necessarily mean putting in place more top-down regulation. A limitation of BitLicense is its attempt to govern a rapidly developing technology with heavy reliance on the legal code. Primavera de Filippi has noted that regulating VCs as though they were a traditional financial product is problematic:

> The challenge is that most regulations today are defined by the product they are meant to regulate. Regulations thus assume a vertical dimension, whereas the innovation brought about by the blockchain has more of a horizontal dimension: it is a cross-cutting innovation that will affect many different sectors of society. And the compartmentalization of this technology into the crypto-currency debate might actually misframe both the challenges and opportunities of this new technology.[29]

The problem is one that is not unique to VCs but applies to digital technology generally. As Nick Grossman of Harvard Business School has written, technology that facilitates decentralised, community-driven networks inherently challenges the assumptions of traditional top-down regulation.[30] According to Grossman, traditional regulation has been permission-based, relying on licensing regimes to authorise or proscribe activity. However, anyone can enter a decentralised network such as Bitcoin. From the perspective of financial crime risk management, this may require acknowledging that technology is reducing barriers to entry in such a way that relying on gatekeepers (such as banks) to permit or restrict access to financial services via traditional KYC approaches is problematic.[31] Indeed, should a terrorist group or another illicit organisation ever succeed in creating its own viable VC, traditional AML/CTF tools would have little relevance;

Announces Approval of First BitLicense Application from a Virtual Currency Firm', press release, 22 September 2015.

27. HM Treasury, *Digital Currencies: Response to the Call for Information*, p. 12.
28. *Ibid.*
29. Primavera de Filippi, 'We Must Regulate Bitcoin. Problem Is, We Don't Understand It', *Wired*, 1 March 2016.
30. Nick Grossman, 'Regulation: The Internet Way: A Data-First Model for Establishing Trust, Safety and Security', Harvard Kennedy School, Ash Center, 28 February 2015.
31. Ariel Deschapell, 'Why Know-Your-Customer Rules Won't Work With Bitcoin', *CoinDesk*, 13 April 2014.

governments would likely need to use cyber warfare methods – such as corrupting software and attacking critical infrastructure – to disrupt them.[32]

Futurist scenarios aside, in the nearer term, VCs challenge certain AML/CTF principles. This does not necessarily require discarding the conceptual frameworks that have driven financial crime risk management to date. However, it may require shifting the emphasis and prioritisation of certain risk management approaches with time. As Joseph Mari suggests, VCs:

> require an evolved approach. This approach needs to utilize existing transaction monitoring, risk rating, and Know Your Customer (KYC) documentation methodologies, and modify them for inclusion of the advances blockchain technology introduces.[33]

What might this involve? Malte Möser and colleagues note that employing KYC at VC exchanges is 'ultimately thwarted by intermediaries who offer [mixing services]', and that other risk management solutions – such as sophisticated transactional analysis – should encompass a greater role in VC risk management.[34] Juan Llanos, an expert on digital payment systems, advocates an approach that places a greater emphasis on 'Know-Your-Funds Flow' – or utilising the data retained on blockchains to enable greater accountability within VC networks.[35]

Some observers argue that traditional KYC methods pose data privacy risks in the context of Bitcoin and other public-ledger-based networks.[36] For example, if a Bitcoin exchange that maintains customers' KYC data is hacked, user personal details could potentially be exposed alongside transactional data that appear on the public blockchain.[37] The BITCRIME Project suggests that the use of KYC with transparent blockchains threatens to undermine 'the protection of personal data of the – mostly – legitimate users who use [cryptocurrencies]'.[38] One alternative to KYC that the BITCRIME Project and some other observers have proposed is transaction 'blacklisting'. In effect, this involves law enforcement labelling specific bitcoins as tainted, given their known involvement in criminal activity, thereby signalling to users in the network that they are to be avoided; VC exchanges would then be prohibited from handling those tainted bitcoins. While this might be seen as a 'reactive' strategy, in that it relies on first identifying criminal activity post-event, rather than attempting to keep criminals out of the system to begin with, the ultimate aim of blacklisting would be to make open blockchain-based cryptocurrencies unattractive to criminals. However, blacklisting is a controversial proposal on

32. Joshua Baron et al., *National Security Implications of Virtual Currency: Estimating the Potential for Non-State Actor Deployment* (Santa Monica, CA: RAND Corporation), pp. 49–58.
33. Joseph Mari, 'When Blockchain, Cryptocurrencies, and AML Meet', *Banking Exchange*, 7 November 2016.
34. Malte Möser et al., 'An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem', eCrime Researchers Summit (2013), p. 2.
35. Juan Llanos, 'Detecting Suspicious Activity on the Bitcoin Blockchain', *Contrarian Compliance blog*, 26 May 2016.
36. Jeni Tennison, 'What is the Impact of Blockchains on Privacy?', *Open Data Institute*, 12 November 2015.
37. Author's discussions with security and data privacy experts, October–November 2016.
38. Rainer Böhme et al., 'Bitcoin and Alt-Coin Crime Prevention: A Recommendation for the Regulation of Virtual Currencies', January 2017, p. 32.

a number of philosophical and technical fronts. As Möser notes, 'the ability to enforce such a blacklisting policy thwarts the very idea of a decentralised currency by projecting power of the legal system into Bitcoin'.[39] Whatever the solution, the point is this: regulators may find that new technology cannot be easily shoehorned into existing frameworks, but that it is regulation that may need to adapt.

This landscape presents a challenge for the public sector, but technological development also presents an opportunity. Increasingly, financial crime experts recognise that the global AML/CTF system is frequently ineffective. As two former US Treasury officials, Juan C Zarate and Chip Poncy, recently noted, 'Current [AML/CTF] efforts are systemically ineffective because of both incomplete implementation and outdated design'.[40] The global AML/CTF regime is a twentieth-century construct that faces irrelevance. Examples of this abound: countries struggling to gather high-quality financial intelligence; regulated firms spending enormous sums on compliance procedures that hinder legitimate business; and the most widely used global payment systems being vulnerable to new crimes, such as cyber theft. With VCs and other fintech innovations, regulators have an opportunity to lay the groundwork for a more effective AML/CTF regime better suited for the twenty-first century.

Whatever specific solutions may emerge, to remain adaptive to technological change, regulation on VCs should be principles-based and dynamic, rather than heavily rules-based and deterministic. This is not to suggest that regulation should be 'light touch' in nature, but rather than relying primarily on specific rules, regulatory approaches of the future might stress that VC platforms – or other new payment platforms more generally – should contain a degree of accountability in their design to enable financial crime risk management, even if that information might be regarded as unconventional under current AML/CTF standards. As Andrew Bailey, Chief Executive of the UK's Financial Conduct Authority (FCA), noted in November 2016, 'a reliance on rule-making by regulators, and therefore the prescription of what cannot be done, can be ill-suited in a world where criminals are able to move very rapidly supported by new technology'.[41] To that end, regulation may need to rely on the ability of technology itself, rather than just the legal code, to embody and reinforce norms.

VCs by their design contain features that can either promote or hinder transparency and privacy, and in doing so can both challenge and enhance AML/CTF efforts. Indeed, it is inaccurate to suggest that in the absence of regulation, VCs operate entirely without constraint. The decentralised networks that use cryptocurrencies operate with rules and incentives that reflect certain communal norms about transparency, consensus, privacy and other issues. These ideas are reflected in the technology itself.

39. Malte Möser et al., 'Towards a Risk Scoring of Bitcoin Transactions', 1st Workshop on Bitcoin Research, 7 March 2014, pp. 1–2.
40. Juan C Zarate and Chip Poncy, 'Designing a New AML System', The Clearing House, <https://www.theclearinghouse.org/research/2016/2016-q3-banking-perspectives/a-new-aml-system>, accessed 17 October 2016.
41. Andrew Bailey, 'Fighting Financial Crime – Looking Forward and Back', speech delivered at the FCA Financial Crime Conference, London, 10 November 2016.

De Filippi refers to this concept as 'governance by design' – or the notion that the norms and rules of a community 'are embedded directly in the underlying technology of the platforms they use to operate'.[42] Jonathan W Lim of the law firm WilmerHale suggests that self-regulatory frameworks, where industry participants operate on agreed norms alongside guidance from regulators, may be more effective than top-heavy regulatory approaches for dynamic products such as VCs.[43] Andres Gardamuz and Chris Marsden define this as a situation where 'governments provide support for mechanisms whereby users of virtual currencies can agree upon and enforce their own "community standards" and rules of conduct'.[44] In a recent example, in November 2016 the Australian Digital Currency and Commerce Association (ADCCA) released a Digital Currency Industry Code of Conduct that includes a pledge by its members to have appropriate AML/CTF procedures. This comes even before Australia has formal VC regulation.[45]

How might self-regulation apply in the case of VCs? One option is as follows: if EU member states find that regulating wallet providers proves difficult in practice, as the VC industry has warned it might, other jurisdictions could instead encourage self-governing AML/CTF approaches rather than formal regulation among wallet providers. This could include encouraging the VC industry to develop voluntary but meaningful standards that encourage responsible AML/CTF practices among custodial wallet providers, but leaves open the question of whether formal AML/CTF regulation is necessary until the sector is more fully developed.

The EU has also discussed another option that contains a self-enforcing component – enabling users of VCs to self-disclose their activity.[46] Under such a system, wallet holders could, for example, choose whether to disclose their activity to authorities, the assumption being that voluntary disclosure would suggest that a user has no intention to conceal any illicit activity. Failure to disclose would not be a crime, and would not necessarily indicate bad intentions, but could provide a sign of potentially higher-risk activity to VC exchanges that encounter those unregistered users. While potentially complex to implement in practice, such a voluntary self-registration scheme might prove an attractive option to explore for countries that wish to encourage transparency but are wary of taking on formal wallet provider regulation.

Self-regulation is not a panacea and has its own challenges. Exempting certain aspects of the VC industry from formal regulation might prove a difficult political sell in many countries, particularly if financial institutions feel the VC industry is being given a free pass. Furthermore,

42. Rachel O'Dwyer interviewing Primavera de Filippi, 'Commons Governance and Law with Primavera de Filippi', *Commons Transition*, 31 July 2015.
43. Jonathan W Lin, 'A Facilitative Model for Cryptocurrency Regulation in Singapore', in David Lee Kuo Chen (ed.), *A Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (Singapore: Elsevier, 2015).
44. Andres Guadamuz and Chris Marsden, 'Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies', *First Monday* (Vol. 20, No. 12, December 2015).
45. ADCCA, 'Australian Digital Currency Industry Code of Conduct', 30 November 2016, <http://adcca.org.au/wp-content/uploads/2016/12/ADCCA-Code-of-Conduct.pdf>, accessed 23 February 2017.
46. See the 5th MLD, which includes discussion of exploring this as a future option, <http://www.bakermckenzie.com/-/media/files/insight/publications/2016/12/report_external_thirdpresidencycompromise_nov16.pdf?la=en>, accessed 1 March 2017.

self-regulation in other contexts has at times proved ineffective. Nonetheless, the broader point remains: new technologies and business models may not always fit comfortably into established paradigms, and innovative approaches – whether self-regulated or otherwise – will be essential to ensuring a balance between managing the risks and harnessing the opportunities of new developments in financial technology.

One sign that some regulators are moving in a future-orientated direction is the use of regulatory 'sandboxes' – or programmes where watchdogs permit new, unlicensed firms to operate and develop new products, services and business models in a safe, monitored environment. The FCA has undertaken a sandbox approach to fintech through Project Innovate, its initiative launched in 2014 to foster competition and innovation among the UK financial sector. Switzerland and Singapore have undertaken sandbox approaches as well,[47] and the UK and Singapore announced plans to form a 'fintech bridge' and jointly facilitate financial innovation.[48] In February 2017, Switzerland announced that it is considering measures that would exempt firms operating with less than 1 million Swiss francs in funds from having to seek authorisation – a measure that could enable small VC firms and other fintechs to 'try out a business model', as the Swiss government puts it, before coming under regulation.[49]

The potential success of sandboxes is still undetermined but offers an indication that the process of trying to evolve regulation alongside technological development in the financial sector is underway.

Observation 2: Development of Knowledge and Expertise

Governments must develop knowledge and expertise on VCs.

Without an adequate understanding of the technology that underlies VCs, public sector staff are unlikely to develop regulatory and investigative approaches that will achieve desired ends. Government officials that do not understand VCs are likely to take misguided steps that can hinder important innovations. VCs also demand that governments possess new types of analytical and forensic tools and have the required skill set to use those tools.

Governments worldwide generally require further expertise and resources. This picture is gradually changing, particularly in the US and across Europe. The US and some EU countries have developed a capacity to seize and confiscate VCs, and are increasingly doing so in cases involving

47. Brian Knight, 'Innovation Will Stall Without a Regulatory Fintech "Sandbox"', *American Banker*, 15 November 2016; Samburaj Das, 'Bitcoin Regulation is on Swiss Government's Fintech-Friendly Agenda', *CryptoCoins News*, 2 November 2016.
48. Kim Jae-kyoung, 'South Korea Urged to Build "Fintech Bridge" with Major Nations', *Korea Times,* 22 June 2016
49. Swiss Federal Council, 'Federal Council Initiates Consultation On New Fintech Regulations', 1 February 2017, <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-65476.html>, accessed 14 February 2017.

bitcoins.[50] Across the US, the UK and Europe, law enforcement agencies are also beginning to use forensic tools and methods designed specifically for detecting activity involving VCs. For example, Europol's European Cybercrime Centre maintains a partnership with Chainalysis to detect cybercrime-related activity.[51] In December 2016, the UN's Office on Drugs and Crime led a training session for law enforcement officers from 34 countries on tracing cybercrime-related activity through the Bitcoin blockchain.[52]

These are important steps, but experts the author consulted in writing this paper suggest that law enforcement capabilities globally will require significant further development to keep pace with the challenge of VCs and their applications in cyberspace.[53] Recognising this need, the US Department of Homeland Security's Science and Technology Directorate launched a programme on anonymous networks and cryptocurrencies. The project aims to improve law enforcement agencies' technical understanding of cryptocurrencies and their applications, and will include the development of new solutions 'to perform forensic analysis of cryptocurrency transactions and facilitate the tracing of currencies involved in illicit transactions'.[54] In February 2017, the Danish government announced it had successfully developed its own blockchain analysis software, which it has used to secure convictions of individuals involved in illicit dark web activity.[55]

It is not only law enforcement bodies that require education. Regulatory agencies in the UK and across the EU should ensure staff have the necessary expertise to understand the operations of those entities they will soon oversee. Staff at financial intelligence units (FIUs), which act as the central repository for all financial intelligence within a country, should have an appropriate understanding of VCs to ensure effective analysis of information. FIUs should aim to develop specialised VC units or working groups. At a global level, organisations such as the Egmont Group of FIUs, which acts as the communications hub for FIUs worldwide, can play an important role in facilitating the exchange of information and knowledge between countries on VCs.

50. William Suberg, 'KYC Dilemma: US Secret Services Seizes $13k from Coinbase Customer', *Bitcoin.com*, 23 July 2016.
51. *Europol*, 'Europol and Chainalysis Reinforce Their Cooperation in the Fight Against Cybercrime', 19 February 2016.
52. Neil Walsh, 'UNODC Cryptocurrency Investigation: Countering Cybercrime, Transnational Organised Crime and Terrorism through the Blockchain', published on LinkedIn, 23 December 2016.
53. Author's discussions with public and private sector experts, October–November 2016.
54. US Department of Homeland Security, 'Anonymous Networks and Currencies', <https://www.dhs.gov/CSD-ANC>, accessed 11 December 2016.
55. Aaron van Wirdum, 'Danish Police Can Now Catch Criminals Who Can Use Bitcoin', *Bitcoin Magazine,* 23 February 2017.

Observation 3: The Value of a Collaborative Approach

Some governments see the value in a collaborative approach with industry. This trend should be adopted more widely.

Governments are realising that they cannot address these issues alone. Partnership with the VC industry is essential to help develop public sector expertise about the legitimate uses of VCs and related technology. Likewise, the VC industry can more effectively combat financial crime if it understands the challenges and perspectives of law enforcement agencies.

The concept of building robust public–private partnerships to enhance AML/CTF efforts is taking hold across the financial sector more generally.[56] With VCs, stakeholders have an opportunity to build public–private partnerships into the fabric of financial crime risk management at an early stage. There are already some initiatives underway.

In September 2016, Europol, Interpol and the Basel Institute on Governance announced the creation of a working group to improve the intelligence picture of VCs.[57] The group will include expert networks with the participation of VC industry representatives. The industry generally welcomed this as an opportunity to demystify VCs for the general public while also enhancing security and legitimacy.[58]

In the US, the Blockchain Alliance is a new VC-focused public–private partnership. Formed in 2015, it includes representatives from around 24 VC firms and numerous US, EU and international law enforcement bodies. It facilitates public–private sector education on financial crime typologies involving Bitcoin, enabling stakeholders to discuss appropriate responses and potential solutions, drawing from ongoing industry and law enforcement challenges.[59]

One limitation of these partnerships is that they do not include exchange of operational information between governments and the private sector on specific criminal targets of interest. With time, it will be important for governments to integrate VCs into operational information-sharing initiatives. The UK, for example, established the Joint Money Laundering Intelligence Task Force (JMLIT), which brings together law enforcement and banks to share information on specific intelligence targets. The UK should consider involving the VC industry in JMLIT to help build a sector-wide picture of illicit financial flows.

56. Clare Ellis and Inês Sofia de Oliveira, 'Tackling Money Laundering: Towards a New Model for Information Sharing', *RUSI Occasional Papers* (September 2015).
57. Europol, 'Money Laundering With Digital Currencies: Working Group Established', press release, 9 September 2016.
58. Iyke Aru, 'How Europol Task Force Will Make Bitcoin Stronger and Will Benefit Users', *CoinTelegraph*, 17 September 2016.
59. Laura Shin, 'How the Blockchain Alliance Helps Law Enforcement With Bitcoin Crime and Developments Like DAO', *Forbes*, 9 August 2016.

Recommendations for Governments

- **Ensure clarity of legal and regulatory frameworks.** Governments should strive for legal and regulatory frameworks that are clear in their intent, scope and wording. Striking a balance between regulation that is clear in its intent but not overly prescriptive will be challenging but is essential.
- **Pursue adaptive, not reactive, regulation.** Governments must be willing to step outside old paradigms of financial crime risk management and consider how technological innovation can reshape traditional AML/CTF practices. Governments should avoid reliance on outdated regulatory frameworks, so an emphasis on accountability over complete control is likely to be most effective. For example, banning highly anonymised cryptocurrencies would likely prove impractical and counterproductive to broader efforts to promote VC innovation; rather, there should be an emphasis on encouraging transparency at certain points of access to those networks.
- **Enhance funding and training.** Governments should ensure staff have adequate knowledge of VCs. This will include training on typologies, related challenges and forensic techniques for detecting financial crime using VCs. Governments should also ensure law enforcement can seize and confiscate VCs. Regional and international forums should include analyst exchange and collaboration efforts.
- **Engage in cross-border coordination.** International organisations, such as FATF and the Egmont Group, should facilitate collaboration between governments on appropriate regulatory and law enforcement responses to VCs. They should encourage and facilitate appropriate information sharing and typology development. Governments should establish region-wide forums for sharing intelligence, resources and forensic solutions. These forums should regularly review approaches to managing VC risks and offer views on their effectiveness. Such efforts should also align closely with international responses to cyber crime and illegal dark web activity.
- **Facilitate a positive role for industry.** Governments should empower the VC industry to play a constructive role in the fight against financial crime. Governments should establish forums for sharing information with the VC industry. In the UK this could, for example, include regular VC industry participation in the JMLIT.

III. The Virtual Currency Industry

This chapter offers observations regarding the VC industry's responses to AML/CTF measures and sets out recommendations for the industry to consider.

Observation 1: Dialogue with the Public Sector

VC industry participants are realising the importance of AML/CTF compliance, but further dialogue with the public sector is necessary.

VC start-up companies and governments may not seem natural allies in the fight against financial crime. At the time of Bitcoin's founding, cryptocurrency developers and enthusiasts were generally hostile to notions that these networks should come under any AML/CTF regulation, and some remain so.

Increasingly, however, many VC start-ups accept that some regulation is here to stay and understand they have a critical role to play. Cases such as the Silk Road and Mt. Gox taught industry that it must work to dispel negative views of VCs.[1] In the UK and the EU, a number of VC exchanges had already developed AML/CTF systems and controls, including KYC procedures, prior to the EU's announcing its intention to draft regulatory measures.[2]

In the US – which clarified in 2013 that it regarded VC exchanges, ATMs and payment processors as regulated money transmitters – VC firms have several years' experience with AML/CTF compliance. Exposure to regulation has made firms in the US sensitive to the risks of non-compliance. In May 2015, US regulators fined Ripple Labs $700,000 for issuing VCs prior to registering as a money transmitter.[3] The message is clear: failure to comply carries real consequences.

Developing robust AML/CTF practices requires considerable time and effort. VC industry participants that come under regulation will inevitably learn by trial and error. This requires an open and candid dialogue both within the VC industry and with regulators.

---

1. Martin Tillier, 'The Two Faces of Bitcoin Regulation', *Nasdaq*, 12 August 2016.
2. UK Digital Currency Association, 'The UK Digital Currency Association's Response to HM Treasury's Digital Currencies: Call for Information', 3 December 2014.
3. US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), 'FinCEN Fines Ripple Labs Inc. for First Civil Enforcement Action Against Virtual Currency Exchanger', press release, 5 May 2015.

Observation 2: An Innovative Approach to AML/CTF

The VC industry is developing bespoke AML/CTF solutions and is unhindered by the legacy systems that drive current inefficiencies among banks and other incumbents.

The VC industry is not merely reacting to government regulation. Rather, some participants are taking a proactive and innovative role in AML/CTF efforts.

A number of firms have developed tools that create an intelligence picture of activity on the Bitcoin blockchain. These rely on transaction analysis that establishes connections between wallet addresses operating across vast networks. This can include the use of 'cluster analysis', which enables the identification of connections between related wallet addresses that a single individual or entity is using. These also include identifying wallet addresses that are linked to dark web activity and tying them to transactions on the blockchain. Law enforcement and VC industry participants are increasingly using a number of these privately developed tools. Well-known providers of such platforms and services include Chainalysis, Elliptic, Confirm and the Blockchain Intelligence Group (BIG).

Firms are also developing novel solutions to the KYC challenges that VCs pose. BIG developed a solution, Bitrank, which provides a risk score for Bitcoin wallets. The tool uses real-time data analytics to provide a view of the likelihood that a wallet could be associated with illicit activity.[4] Elliptic is partnering with LexisNexis to develop KYC solutions for the Bitcoin network too.[5] A number of firms are developing methods for individuals to maintain encrypted data on the blockchain in a manner that would enable a degree of anonymisation while also ensuring firms have access to up-to-date and reliable KYC information.[6] As one observer describes it:

> The blockchain would in effect maintain a record of various ID credentials for an individual and act as a trusted pseudonym for someone's identity … The details of these credentials – the real identity – would only ever be released under prescribed, specific circumstances … So while the Bitcoin operator might not know who owns a particular wallet … it would know for sure that another regulated institution does and, more importantly, that regulators can find out if needs be.[7]

Traceability of transactions remains possible as long as Bitcoin dominates among cryptocurrencies in its current form. Further adoption of anonymising techniques could hinder transactional analysis. However, some developers of altcoins that feature greater anonymity than Bitcoin are innovating customised AML/CTF solutions. In September 2016, founders of the altcoin Dash – which stands for 'digital cash' – announced their partnership with Coinfirm.

4. Blockchain Intelligence Group, <https://blockchaingroup.io/>, accessed 23 February 2017.
5. Jemima Kelly, 'LexisNexis Risk Solutions and Start-Up Join to Curb Money Laundering in Bitcoin', *Reuters*, 3 August 2016.
6. Michael Scott, 'Kyckr's Rob Leslie on Blockchain and Regulatory Compliance', *Bitcoin Magazine*, 26 September 2016.
7. *Signicat*, 'Will the 4th AML Directive be a Blessing or a Blow for Bitcoin?', <https://www.signicat.com/eid/aml-directive-bitcoin/>, accessed 23 February 2017.

According to Dash's developers, the partnership will enable 'the first interwoven solution for AML/KYC compliance in cryptocurrency'.[8] Dash relies on technology similar to Monero and Zcash, ensuring details of its blockchain's activity can remain hidden from public view; however, the Coinfirm solution will enable ongoing monitoring of the Dash blockchain where users have contact with VC exchanges or other regulated institutions. The solution uses multisource data analytics to enable real-time risk scoring and monitoring of counterparts' activity.[9]

These developments demonstrate that the VC industry is in a position to reshape the future of AML/CTF efforts. VC start-ups have an advantage over banks and the traditional financial sector because they are unencumbered by inefficient legacy systems and outdated compliance processes. Rather, VC innovators are in a position to build novel and efficient AML/CTF solutions into their platforms from the outset. If combined with an adaptive and forward-looking regulatory mindset, such innovation could enable a more dynamic, technology-driven approach to combating financial crime.

Observation 3: Intra-Industry Interaction on AML/CTF

Some in the VC industry are learning to value collaborative AML/CTF approaches; stakeholders would benefit from more frequent intra-industry interaction to foster AML/CTF best practices.

As noted earlier, initial efforts are underway to develop sustained AML/CTF public–private partnerships.[10] The VC industry would also benefit from greater intra-industry collaboration. Tim Swanson of the financial services technology innovation consortium R3 notes that public–private partnerships on VCs at present have 'limited capabilities … [and] fail to plug the KYC/AML gaps … Right now there is no global, industry standard for "best practices" in mutualizing, implementing, or carrying out KYC / AML provisions for cryptocurrencies'.[11]

Industry participants can work together to ensure their AML/CTF efforts are effective and coherent. Establishing regular intra-industry forums to allow VC exchanges to share their experience of financial crime risk management practices and solutions could allow industry participants to determine what works, what does not, and how the industry can evolve.

Several VC industry associations and advocacy groups already exists, such as Coin Center in the US. However, the industry would benefit from visible AML/CTF-focused bodies that enable

8. *Finextra*, 'Dash Adds Full Support for AML/KYC Compliance With Coinfirm', 28 September 2016; Dash, 'Exploring Compliance on the Dash Blockchain', <https://www.dash.org/news/exploring-compliance-on-the-dash-blockchain/>, accessed 11 December 2016.
9. Bitcoin.com forum, 'Everything You Want to Know About Coinfirm's Dash Integration for AML/KYC Compliance', 12 October 2016, <https://forum.bitcoin.com/dash/everything-you-want-to-know-about-coinfirm-s-dash-integration-for-aml-kyc-compliance-t11540.html>, accessed 11 December 2016; Michael Scott, 'Interview: Dash and Coinfirm on Digital Currency Compliance Partnership', *Bitcoin Magazine*, 7 October 2016.
10. Author's discussions with industry experts, October–November 2016.
11. Tim Swanson, 'A Kimberley Process for Cyrptocurrencies', Great Wall of Numbers: Business Opportunities and Challenges in Emerging Markets, 27 June 2016.

collaboration among members specifically on financial crime risk management and compliance challenges, and that provide for industry white papers and other publicly available information on best practice approaches.

Recommendations for Industry Participants

- **Continue to take an innovative, entrepreneurial approach to developing AML/CTF solutions.** VC industry participants should continue to explore the potential for increasingly sophisticated tools and applications for managing financial crime risk. Innovators should aim to achieve an appropriate balance between data privacy and transparency.
- **Establish intra-industry working groups.** Collaborative exchanges are vital to ensure that industry participants can tackle AML/CTF challenges. Stakeholders should create formal collaborative working groups and associations that enable them to exchange information on best practices and risk management solutions in the sector.

IV. Banks and the Established Financial Sector

This chapter offers observations regarding the incumbent financial sector's response to VCs and sets out recommendations for financial sector stakeholders.

Observation 1: The Future of Relations Between Banks and the VC Industry

The relationship between banks and the VC industry remains a complex one, and the future is still unclear, but some banks see value in VCs and related technology.

Banks and other incumbent financial institutions have often viewed VCs sceptically. Banks are the target of VC developers' disruptive aims, so this is hardly surprising. But banks have also expressed legitimate concerns about the financial crime risks that VC firms can pose.

One place where banks interact with the VC industry is where cryptocurrency exchanges require accounts to serve their customers' fiat currency trading needs. Many banks have proceeded cautiously before opening accounts for VC exchanges; some refuse to do so at all due to potential risks.[1] Those banks that do provide services for VC exchanges generally regard that business as higher risk and expect them to have robust AML/CTF compliance practices in place. This incentivises VC industry to take financial crime risk management seriously.

Despite their concerns about the VC industry, banks remain interested in the underlying technology and its potential applications. In particular, banks are exploring how to harness DLT to enhance financial services by streamlining processes that are currently heavily fragmented. A number of banks are undertaking projects to explore the applications of blockchain in correspondent banking, trade finance, syndicated lending and other areas of financial services. Banks also see in DLT the potential to streamline KYC practices by offering centralised repositories for secure customer information that can be updated in real time and shared among financial institutions, versus the current manual-intensive process of collecting separate information on customers bank by bank.[2]

The most publicised attempt by the banking sector to explore the frontiers of DLT is the R3 consortium. R3 is a self-described 'blockchain-inspired' partnership of more than 50 financial institutions that collaborate to design and develop shared applications. This includes the

1. See Pratin Vallabhaneni et al., 'Overcoming Obstacles to Banking Virtual Currency Businesses', Coin Center Report, May 2016; Paris Cowan, 'Aussie Banks Dump Bitcoin Traders', *Itnews*, 8 April 2015.
2. Nicholas Elliott, 'The Morning Risk Report: How Blockchain Might Be Used in Compliance', *Wall Street Journal*, 2 December 2016.

development of R3's own platform, known as Corda, for executing smart contracts and other applications.[3] A number of banks involved in R3 have also experimented with DLT via Ripple, a start-up payment protocol and platform that aims to replace slower cross-border settlement methods. Ripple facilitates real-time payment settlement using DLT with its own cryptocurrency, known as XRP.

The ultimate success of these initiatives is yet to be determined – though recently they have shown signs of growing pains. In late 2016, a number of banks withdrew from the R3 consortium, suggesting divergence in the sector about the most appropriate uses of DLT and how to harness those uses.[4]

Some observers remain skeptical of what they perceive as 'blockchain hype' and regard the banking sector's recent attempts to explore the use of blockchains without simultaneously embracing VCs as misplaced.[5] According to this view, the incentives from cryptocurrency mining provide the only viable mechanism for maintaining a blockchain, which should remain decentralised, and banks' efforts to develop private blockchains without similar open structures are futile.[6] Some VC enthusiasts see this as a sign that banks should keep their hands off disruptive VCs and related technology all together.

Other observers suggest that banks would be better served to focus their attention not only on DLT, but on eventually providing VC services as well. As Sarah Fielder and Jeremy Light of the consulting firm Accenture suggest, '[b]anks should therefore start thinking about the services to provide retail and corporate customers using … cryptocurrencies, should the market shift in this direction, covering both retail and corporate customers' cryptocurrency payment'.[7] How banks resolve this could influence whether VCs achieve greater widespread adoption.

A number of banks are already exploring ways to offer their own cryptocurrency services to customers. To date, many regulatory agencies have discouraged or prohibited established financial institutions from dealing in VCs. The EBA, for example, advised in 2014 that EU member states should prevent their banks from transacting in VCs or enabling VC transactions in the absence of regulation[8]. However, some banks further afield are intent on offering such services. In November 2016, a South Korean bank, Shinhan Bank, announced its intention to start a cryptocurrency remittance service to China.[9] Some observers suggest that banks could

3. Richard Gendal Brown, 'Introducing R3 Corda: A Distributed Ledger Designed for Financial Services', 5 April 2016.
4. Alexander J Martin, 'R3 Four Flew: What's Driving Banks to Flee Blockchain Consortium?: Too Big to Fail or Too Big to Work?', *The Register*, 29 November 2016.
5. Author's discussions with VC industry experts, December 2016.
6. Jeff John Roberts, 'The Crisis in Bitcoin and the Rise of Blockchain', *Fortune*, 4 March 2016.
7. Sarah Fielder and Jeremy Light, 'Distributed Consensus Ledgers for Payments', Accenture Payment Services: Everyday Bank Research Series, 2015, p. 13.
8. Avaneesh Pandey, 'EBA Advises European Banks Against Using Bitcoin and Virtual Currencies', *International Business Times*, 4 July 2014.
9. Chung Ji-sung, 'Shinhan Bank to Launch its First Digital Currency Remittance Service in Dec', *Pulse*, 4 November 2016.

someday offer wallet services, cryptocurrency deposit taking services, cross-border payment settlement and ATM access.[10]

Observation 2: Banks Also Seek Innovative AML/CTF Approaches

Established financial sector participants and the VC industry share an interest in improving the global AML/CTF regime.

The VC industry wants to be seen as respectable among the general public, and banks want to harness VC-related technology. Consequently, both have an interest in finding workable AML/CTF strategies that enable them to further joint interests. Banks therefore should not treat the VC industry as a problem; and the industry should not treat banks as a nuisance. VC firms should be receptive to banks' concerns about risk; and banks should openly recognise that the VC industry possesses valuable technical solutions and knowledge. In one recent example of positive cross-sector interaction, Barclays entered into an arrangement with Chainalysis to assist the lender in taking on Bitcoin exchanges as clients.[11]

More broadly, both the traditional financial sector and the VC industry would benefit from an improved global approach to combating financial crime. Banks have in numerous instances been the deserving recipients of large fines and penalties for breaches of their AML/CTF obligations. However, banks have also experienced firsthand that many existing AML/CTF measures are often ineffective. In February 2017, The Clearing House, an association of major US banks, published a report calling for a major overhaul of US AML/CTF approaches, claiming that '[t]he current AML/CFT statutory and regulatory framework is outdated and thus ill-suited for apprehending criminals and countering terrorism in the 21st century'.[12]

Banks and the VC industry should partner to develop solutions for improving AML/CTF practices. Banks are in a position to share their experiences in AML/CTF risk management with the VC industry, and have resources to invest in new solutions; the VC industry possess the technological know-how to contribute innovative approaches.

10. Fielder and Light, 'Distributed Consensus Ledgers for Payments', p. 13.
11. Pete Rizzo, 'Chainalysis: Barclays Deal is Start of Banks Opening Up to Bitcoin', *CoinDesk*, 14 October 2015.
12. The Clearing House, 'A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Law Enforcement', February 2017, p. 4.

Recommendations for Banks and Other Established Financial Sector Participants

- **Build knowledge and awareness of VCs**. Firms in the established financial sector should ensure staff understand VCs, their applications and related risks.
- **Establish AML/CTF partnerships with the VC industry.** Banks should work with the VC industry to establish formal cross-sector partnerships aimed at building strong financial crime risk management practices related to VCs and DLT applications. This could occur bilaterally, as between Barclays and Chainalysis, or more broadly, for example through formal networking arrangements, working groups or associations.

V. Conclusions

VCs AND RELATED technology present a challenge for the public and private sectors. On the one hand, the financial crime risks VCs pose are real, even if they are still immature and evolving. Established criminal and terrorist organisations have yet to use cryptocurrencies on a widespread scale, but as the scope of their involvement in online crime grows, the use of cryptocurrencies by these actors could expand. Cybercriminals are increasingly turning to cryptocurrencies in their operations, demanding new law enforcement approaches and techniques.

On the other hand, VCs and related technology – particularly DLT – offer a number of potential benefits. For example, they could contribute to financial inclusion and make the delivery of financial services more efficient and effective. Governments must be careful not to stifle these innovations.

Governments should also see in VCs an opportunity to improve financial crime risk management. VC-related technology offers the prospect of new solutions and techniques for combating financial crime. Governments should look to VCs as a test case for developing new and more effective AML/CTF approaches that also respect the need for financial privacy and innovation. This will require dynamic regulatory frameworks.

The private sector has an indispensable role in this effort. The VC industry can innovate technical solutions and best practices. Banks and the incumbent financial sector can contribute valuable resource and experience towards developing related technology and concurrent financial crime risk management practices.

By taking an approach that is forward-looking, adaptive, collaborative and innovative, stakeholders can both manage the challenges and harness the opportunities of VCs.

About the Author

David Carlisle is an independent consultant who previously worked with the US Department of the Treasury's Office of Terrorism and Financial Intelligence. He has conducted research for RUSI's Centre for Financial Crime and Security Studies (CFCS) on improving financial intelligence. David has lived and worked in London since 2012.