STUDY

Requested by the TAX3 committee

European Parliament

Cryptocurrencies and blockchain

Legal context and implications for financial crime, money laundering and tax evasion

Policy Department for Economic, Scientific and Quality of Life Policies
Authors: Prof. Dr. Robby HOUBEN, Alexander SNYERS
Directorate-General for Internal Policies
PE 619.024 - July 2018

EN

Cryptocurrencies and blockchain

Legal context and implications for financial crime, money laundering and tax evasion

Abstract

More and more regulators are worrying about criminals who are increasingly using cryptocurrencies for illegitimate activities like money laundering, terrorist financing and tax evasion. The problem is significant: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide. This paper prepared by Policy Department A elaborates on this phenomenon from a legal perspective, focusing on the use of cryptocurrencies for financial crime, money laundering and tax evasion. It contains policy recommendations for future EU standards.

This document was requested by the European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance.

AUTHORS
Prof. Dr. Robby HOUBEN, University of Antwerp, Research Group Business & Law, Belgium.
Alexander SNYERS, University of Antwerp, Research Group Business & Law, Belgium.

ADMINISTRATOR RESPONSIBLE
Dirk VERBEKEN

EDITORIAL ASSISTANT
Janetta CUJKOVA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Economic, Scientific and Quality of Life Policies
European Parliament
B-1047 Brussels
Email: Poldep-Economy-Science@ep.europa.eu

Manuscript completed in June 2018

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

CONTENTS

LIST OF ABBREVIATIONS

AMLD1	First Anti-Money Laundering Directive
AMLD2	Second Anti-Money Laundering Directive
AMLD3	Third Anti-Money Laundering Directive
AMLD4	Fourth Anti-Money Laundering Directive
AMLD5	Fifth Anti-Money Laundering Directive
BIS	Bank for International Settlements
CPMI	Committee on Payments and Market Infrastructures
DAC5	Fifth revision of the Directive on administrative cooperation in taxation
DLT	Distributed ledger technology
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
FATF	Financial Action Task Force
FIU	Financial intelligence unit
FTR	Funds Transfer Regulation
IMF	International Monetary Fund
ITO	Initial Token Offering
MTF	Multilateral trading facility
OTF	Organised trading facility
P2P	Peer to Peer
PoS	Proof of Stake

PoW	Proof of Work
PSD2	Second revision of the Directive on Payment Services

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

More and more regulators are worrying about criminals who are increasingly using cryptocurrencies for illegitimate activities like money laundering, terrorist financing and tax evasion. The problem is significant: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide.[1] This research elaborates on this phenomenon, focusing on the use of cryptocurrencies for financial crime, money laundering and tax evasion.

The key issue that needs to be addressed is the anonymity surrounding cryptocurrencies. This anonymity, varying from complete anonymity to pseudo-anonymity, prevents cryptocurrency transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter and criminal organisations to use cryptocurrencies to obtain easy access to "clean cash". Anonymity is also the major issue when it comes to tax evasion. When a tax authority does not know who enters into the taxable transaction, because of the anonymity involved, it cannot detect nor sanction this tax evasion.

The existing European legal framework is failing to deal with this issue. There are simply no rules unveiling the anonymity associated with cryptocurrencies. However, the tide is changing. The fifth revision of the directive on money laundering and terrorist financing, AMLD5, is in the final phase of being adopted. AMLD5 includes a definition of virtual currencies and subjects virtual currency exchange services and custodian wallet providers to customer due diligence requirements and the duty to report suspicious transactions to financial intelligence units. The information obtained, can also be used by tax authorities to combat tax evasion.

AMLD5's definition of virtual currencies is sufficient to combat money laundering, terrorist financing and tax evasion via cryptocurrencies. Nevertheless, it is important to closely follow-up on the use cases of virtual currencies to ascertain that the definition remains to be a sufficient one going forward.

When we look at the key players in cryptocurrency markets, we can see that a number of those are not included in AMLD5, leaving blind spots in the fight against money laundering, terrorist financing and tax evasion. The examples are numerous and include miners, pure cryptocurrency exchanges that are not also custodian wallet providers, hardware and software wallet providers, trading platforms and coin offerors. Persons with malicious intent could look up these blind spots. If that would happen and it would appear to have a (material) adverse effect on the fight against money laundering, terrorist financing and tax evasion, expanding the scope of AMLD5 should be considered.

With respect to unveiling the anonymity of users in general (i.e. also outside of the context of virtual currency exchanges and custodian wallet providers), no immediate action is taken. Only in its next supranational risk assessment, the Commission will assess a system of voluntary registration of users. This approach is not very convincing if the legislator is truly serious about unveiling the anonymity of cryptocurrency users to make the combat against money laundering, terrorist financing and tax evasion more effective. A mandatory registration and a pre-set date as of which it applies, would be a better approach, albeit of course more intrusive. For reasons of proportionality, mandatory registration could be made subject to a materiality threshold.

[1] COMMISSION STAFF WORKING DOCUMENT 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/2016/0223 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN.

For some aspects relating to some cryptocurrencies a ban should be considered. To mind come the features that are designed to make cryptocurrency users untraceable. Why is such degree of anonymity truly necessary? Would allowing this not veer too far towards criminals? In any event, imposing a ban should always be focused on specific aspects facilitating the illicit use of cryptocurrency too much.

The European level is appropriate to address money laundering, terrorist financing and tax evasion via cryptocurrencies. Even more appropriate is the international level, as crypto activity is not limited by the European border. International collaboration is crucial to successfully impose and enforce rules on combating money laundering, terrorist financing and tax evasion. From a regulatory perspective, the ongoing G20 attention paid to regulating cryptocurrencies is therefore welcome.

As regards blockchain, it would be too blunt to associate blockchain with money laundering, terrorist financing or tax evasion. It is just technology, on which a large number of cryptocurrencies run, but which is not designed to launder money, facilitate terrorist financing or evade taxes. Blockchain has numerous applications throughout the whole lawful economy. It would not be wise to discourage future innovations in this respect by submitting blockchain and fintech's exploring its use cases to burdensome requirements, simply because of one of the applications using blockchain technology, cryptocurrencies, is used illicitly by some. Therefore, blockchain should be left untouched from a money laundering, terrorist financing and tax evasion perspective. The fight against money laundering, terrorist financing and tax evasion should focus on the illicit use cases of cryptocurrencies.

1. GENERAL INFORMATION

KEY FINDINGS

- The key issue that needs to be addressed in the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies is the anonymity surrounding cryptocurrencies.
- The existing European legal framework is failing to deal with this issue.
- The tide is changing: the fifth revision of the directive on money laundering and terrorist financing, AMLD5 includes a definition of virtual currencies and subjects virtual currency exchange services and custodian wallet providers to customer due diligence requirements and the duty to report suspicious transactions to financial intelligence units.
- A number of key players in cryptocurrency markets are not included in the scope of AMLD5, leaving blind spots in the fight against money laundering, terrorist financing and tax evasion.
- With respect to unveiling the anonymity of users in general, no immediate action is taken. The Commission will assess only in its next supranational risk assessment a system of voluntary registration of users. A mandatory registration and a pre-set date as of which it applies would be a better approach to unveil the anonymity of cryptocurrency users.
- For some aspects relating to some cryptocurrencies a ban should be considered.
- The European level is appropriate to address money laundering, terrorist financing and tax evasion via cryptocurrencies, but even more more appropriate is the international level, as crypto activity is not limited by the European border.
- Blockchain is technology, on which a large number of cryptocurrencies run, but which is not designed to launder money, facilitate terrorist financing or evade taxes. Blockchain has numerous applications throughout the whole lawful economy. The fight against money laundering, terrorist financing and tax evasion should focus on the illicit use cases of cryptocurrencies and not on blockchain.

1.1. Background

With the growing popularity of the crypto market, the large number of unregulated cryptocurrencies (several hundreds), greater attention is now being paid by governments and other stakeholders around the world. Illustrative is that the total market capitalisation of the 100 largest cryptocurrencies is reported to exceed the equivalent of EUR 330 billion globally by early 2018. The total market capitalisation of all cryptocurrencies together in that period peaked at an even higher USD 728 billion, dropping just three weeks later to approximately USD 360 billion.[2] Regulators are looking at whether — and how — to regulate cryptocurrencies. Up till now there is no univocal view on how to do that. In any event, there are compelling reasons why cryptocurrencies should be under more

[2] R.M. BRATSPIES, "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 6-7 (electronically available via https://ssrn.com/abstract=3141605).

scrutiny by regulators and supervisors. The threat of price volatility, speculative trading, hack attacks, money laundering and terrorist financing all call for stricter regulation.

This research deep dives into the latter issue. According to many, aside from the instability of cryptocurrency prices, these cryptocurrencies must have greater regulatory oversight in order to prevent illegal activity and illegitimate use. Aside from the instability of cryptocurrency prices, regulators are worrying about criminals who are increasingly using cryptocurrencies for activities (trading away from official channels) like fraud and manipulation, tax evasion, hacking, money laundering and funding for terrorist activities. The problem is a significant one: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide.[3]

1.2. Scope of the research

Cryptocurrencies and blockchain are a monstrous topic. There are several hundreds of cryptocurrencies and the applications of blockchain technology are also numerous. To make this research a useful and focused one, we have to narrow it down. To do this, the research attaches to multiple connecting factors, defining its scope.

Firstly, the research is limited to *cryptocurrencies and blockchain*. This means that other types of assets than cryptocurrencies, such as tokens or crypto securities, are not within the scope of this research. We will explain how these assets differ from cryptocurrencies further on. We will also not elaborate on derivatives of cryptocurrencies, which are essentially investment instruments. Blockchain will be scrutinized to the extent cryptocurrencies run on this technology. Therefore, blockchain technology will not be looked at outside of the context of cryptocurrencies, such as it being used as a technique to eliminate intermediaries in the financial, public or other sector. This would lead to far and exceeds the scope of this research.

Secondly, the research relates to the *legal context* of cryptocurrencies and blockchain. The focus is, hence, a legal one. This means that we will not elaborate on all the technical aspects – and there are many – relating to cryptocurrencies and blockchain. We will only touch upon those to the extent necessary to understand the legal context. We will also not take an economic, criminological or any other approach than a legal one. We focus on the *EU* legal context. Therefore, we will not elaborate on the international[4] or national context, unless it is relevant to better understand the European context.

Thirdly, the legal context is addressed *in connection with the implications for* financial crime, money laundering and tax evasion. Therefore, we will only scrutinize the legal context of cryptocurrencies and blockchain to the extent relevant in connection with financial crime, money laundering and tax evasion. We will do this by assessing what exactly cryptocurrencies and blockchain are, which challenges they bring from the perspective of combating financial crime, money laundering and tax evasion, to which extent they are caught by legislation at European level and what could be done to improve the legal framework. We will not deep dive into other legal queries than those related to

---

[3] COMMISSION STAFF WORKING DOCUMENT 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/2016/0223 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN.

[4] See for a number of examples on non-EU measures on cryptocurrencies: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 47-50 (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf). See also: P. VALENTE, "Bitcoin and Virtual Currencies Are Real: Are Regulators Still Virtual?", INTERTAX, Volume 46, Issue 6 & 7, 546-547.

money laundering, terrorist financing and tax evasion, such as the qualification of cryptocurrencies under tax laws or the protection of investors in cryptocurrencies (whether or not consumers) under financial services laws.[5] Although very interesting, these queries exceed the scope of this research.

Lastly, the research relates to *financial crime, money laundering and tax evasion*. Financial crime is no term of art. Generally speaking, it is used as an umbrella term to designate all sorts of crimes relating to the use of finances, such as fraud, theft, tax evasion, bribery, money laundering, terrorist financing, etc.. In an EU context, financial crime includes *inter alia* crimes against the integrity of the financial sector, such as money laundering and insider dealing, and crimes against the financial interest of the Union, such as fraud. In this research we will not elaborate on all imaginable financial crimes. On the contrary, we will focus on money laundering, terrorist financing and tax evasion as subtypes of financial crime. This focus can be justified for a number of reasons. Firstly, money laundering, terrorist financing and tax evasion are at the forefront of the EU's efforts on combating financial crime.[6] Furthermore, the EU is clearly taking the approach to address cryptocurrency issues via anti-money laundering and counter terrorism financing legislation. This research acknowledges that approach and takes the same one. Secondly, leaving theft aside, money laundering, terrorist financing and tax evasion are probably the three types of financial crimes that are likely to be most associated with cryptocurrencies and blockchain, *i.e.* when persons commit a crime relating to cryptocurrencies and blockchain, the likelihood of that crime being money laundering, terrorist financing and/or tax evasion is high. Cryptocurrencies are thought to be very suitable for money laundering, terrorist financing and tax evasion purposes because of their anonymity, cross-borders nature and quick transferability[7]. Thirdly, some crimes simply cannot be committed at this stage via cryptocurrencies. Financial crimes such as market abuse and insider dealing are for instance of no relevance for cryptocurrencies. Market abuse rules relate to financial instruments traded on a regulated market, a multilateral trading facility ("***MTF***") or an organised trading facility ("***OTF***"). For the application to cryptocurrencies this poses two problems: cryptocurrencies are not financial instruments and they are not traded on a regulated market, MTF or OTF.

The research starts with a definition of cryptocurrencies and blockchain. After that, a taxonomy of cryptocurrencies will be given on the basis of an analysis of the 10 cryptocurrencies with the highest market capitalisation. This taxonomy will serve as a benchmark throughout this research and will allow to verify the adequacy of the existing and upcoming legal framework.

This study has been completed on 20 June 2018.

---

5 Another interesting query, which we will also not deep dive into in the context of this study, is how cryptocurrencies affect monetary policy. For more information on this topic we refer to: D. HELLER, "The implications of digital currencies for monetary policy", in-depth analysis commissioned by the Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, May 2017, 12p. (electronically available via http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL_IDA(2017)602048_EN.pdf).

6 See e.g. E. HERLIN-KARNELL and N. RYDER, "The robustness of EU Financial Crimes Legislation: A Critical review of the EU and UK Anti-Fraud and Money Laundering Scheme", 2017, European Business Law Review, No. 4, 1-39.

7 See e.g. S. ROYER, "Bitcoins in het Belgische strafrecht en strafprocesrecht", *RW* 2016-17, No. 13, 486.

1.3. Overview of policy recommendations for future EU standards

This study sets out a number of policy recommendations for future EU standards. The main ones are outlined below.

Policy recommendations for future EU standards

- To unveil the anonymity of cryptocurrency users the EU should consider a system of mandatory registration of users and a pre-set date as of which it applies rather than a system of voluntary registration of users.
- The EU should also think about expanding the list of "obliged entities" under AMLD5 with those players that are identified in this study as the weak spots or have great potential of being weak spots, including miners, pure cryptocurrency exchanges that are not also custodian wallet providers, software and hardware wallet providers, trading platforms and coin offerors.
- Furthermore, the EU should think about imposing a specific ban on such aspects surrounding cryptocurrencies that are aimed at making it impossible to verify their users (e.g. mixing) and criminally sanctioning these aspects.
- In addition, the EU could consider extending the scope of the Funds Transfer Regulation to make sure that all relevant information accompanying cryptocurrency transactions is there, allowing an adequate money laundering and terrorist financing check. The entities that would have to fulfil the requirements could be the intermediaries through which the transactions run.
- In the longer term, the EU should consider developing a tailored and more comprehensive framework for cryptocurrencies, and setting EU standards for cryptocurrencies in line with suggestions and recommendations made by the EBA, including license requirements for cryptocurrency service providers. Part of such framework could be to create or impose a "middleman", where the use of blockchain or other distributed ledger technology has cut out such middleman, as this will allow the regulator to attach regulation to an identifiable person, thus contributing to enhanced compliance and effective enforcement.
- With a view of achieving unified regulation of cryptocurrencies at G20 level, it is recommended that the EU leads further initiatives by example.
- The EU should leave blockchain be from a money laundering, terrorist financing and tax evasion perspective and focus on the illicit use cases of cryptocurrencies. Blockchain is just technology and can have beneficial effects in a wide array of sectors. Its development as such should not be discouraged.

2. CRYPTOCURRENCIES AND BLOCKCHAIN

2.1. What is blockchain?

2.1.1. Defining blockchain: a technology with many faces

Blockchain is a particular type or subset of so-called distributed ledger technology ("***DLT***").[8] DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes.[9]

Blockchain is a mechanism that employs an encryption method known as cryptography[10] and uses (a set of) specific mathematical algorithms to create and verify a continuously growing data structure – to which data can only be added and from which existing data cannot be removed – that takes the form of a chain of "transaction blocks"[11], which functions as a distributed ledger.[12]

In practice, blockchain is a technology with many "faces". It can exhibit different features and covers a wide array of systems that range from being fully open and permissionless, to permissioned[13]:

- On an *open, permissionless blockchain*, a person can join or leave the network at will, without having to be (pre-)approved by any (central) entity.[14] All that is needed to join the network and add transactions to the ledger is a computer on which the relevant software has been installed. There is no central owner of the network and software, and identical copies of the ledger are distributed to all the nodes in the network.[15] The vast majority of cryptocurrencies currently in circulation is based on permissionless blockchains (e.g. Bitcoin, Bitcoin Cash, Litecoin, …).
- On a *permissioned blockchain*, transaction validators (i.e. nodes) have to be pre-selected by a network administrator (who sets the rules for the ledger) to be able to join the network.[16] This allows, amongst others, to easily verify the identity of the network participants.[17] However, at the same time it also requires network participants to put trust in a central coordinating entity to

---

8 Another example of distributed ledger technology is "*directed acyclic graph*", the underlying technology of the IOTA-platform (see below). See also: M. VAN DE LOOVERBOSCH, "Crypto-effecten: tussen droom en daad", TRV-RPS 2018, 193, footnote 2.

9 See: World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 1. See also: CPMI, "Digital currencies", November 2015, https://www.bis.org/cpmi/publ/d137.pdf, 5.

10 This technique is discussed and defined further below.

11 Hence the name "blockchain".

12 See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 1.

13 Some authors also distinguish so-called "consortium blockchains", which operate as closed, cryptographically secured databases (i.e. the ledger can only be accessed by the nodes that are participating in the network and different rules apply on who can update the state of the ledger). *Inter alia:* P. WITZIG and V. SALOMON, "Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry", Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf, 7.

14 World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 1.

15 *Ibid.*

16 Permissioned blockchains are built so that "*they grant special permissions to each participant for specific functions to be performed—like read, access and write information on the blockchains*" (hence the name "permissioned" blockchains). See: S. SHOBHIT, "Public, Private, Permissioned Blockchains Compared", April 2018, https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/.

17 World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 11.

select reliable network nodes.[18] In general, permissioned blockchains can be further divided into two subcategories. On the one hand, there are *open or public permissioned blockchains*, which can be accessed and viewed by anyone, but where only authorised network participants can generate transactions and/or update the state of the ledger.[19] On the other hand, there are *closed or "enterprise" permissioned blockchains*[20], where access is restricted and where only the network administrator can generate transactions and update the state of the ledger.[21] What is important to note is that just like on an open permissionless blockchain, transactions on an open permissioned blockchain can be validated and executed without the intermediation of a trusted third-party. Some cryptocurrencies, like Ripple and NEO utilise public permissioned blockchains.[22]

2.1.2. How a blockchain works: the basics

a. The blockchain is a distributed database

In simple terms, the blockchain can be thought of as a distributed database. Additions to this database are initiated by one of the members (i.e. the network nodes), who creates a new "block" of data, which can contain all sorts of information. This new block is then broadcasted to every party in the network in an encrypted form (utilising cryptography) so that the transaction details are not made public.[23] Those in the network (i.e. the other network nodes) collectively determine the block's validity in accordance with a pre-defined algorithmic validation method, commonly referred to as a "consensus mechanism"[24]. Once validated, the new "block" is added to the blockchain, which essentially results in an update of the transaction ledger that is distributed across the network.[25]

In principle, this mechanism can be used for any kind of value transaction and can be applied to any asset that can be represented in a digital form[26]. We illustrate this in Figure 1 below.

b. Transaction "blocks" are signed with a digital signature using a private key

Every user on a blockchain network has a set of two keys. A private key, which is used to create a digital signature for a transaction, and a public key, which is known to everyone on the network. A

---

18 *Ibid.*

19 P. WITZIG and V. SALOMON, "Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry", Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf, 6-7.

20 These blockchains are sometimes also referred to as "private blockchains". See *Inter alia:* P. JAYACHANDRAN, "The difference between public and private blockchain", May 2017, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/; S. SHOBHIT, "Public, Private, Permissioned Blockchains Compared", April 2018, https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/; P. WITZIG and V. SALOMON, "Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry", Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf, 7.

21 P. WITZIG and V. SALOMON, "Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry", Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf, 6-7.

22 Also see below under 3.2.9 NEO (NEO).

23 World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 1.

24 *Ibid.*, 1. Also see below 2.1.3. The blockchain consensus mechanisms.

25 CPMI, "Digital currencies", November 2015, https://www.bis.org/cpmi/publ/d137.pdf, 5.

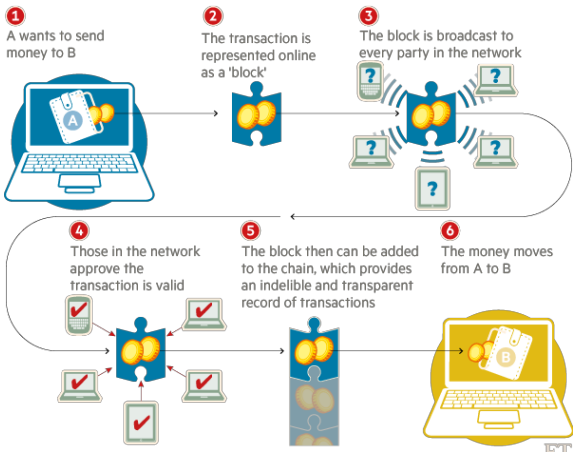
26 See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 1.

public key has two uses: 1) it serves as an address on the blockchain network; and 2) it is used to verify a digital signature / validate the identity of the sender.[27]

On the Bitcoin blockchain, this translates into the following example. Suppose that Anna wants to send 100 Bitcoins to Jeff, then first of all she will have to digitally sign this transaction using her private key (which is only known to her). She will have to address the transaction to Jeff's public key, which is Jeff's address on the Bitcoin network. Next, the transaction, which will be collated into a "transaction block", will have to be verified by the nodes within the Bitcoin network. Here, Anna's public key will be used to verify her signature. If Anna's signature is valid, the network will process the transaction, add the block to the chain and transfer 100 Bitcoins from Anna to Jeff.

A user's public and private keys are kept in a digital wallet or e-wallet. Such wallet can be stored or saved online (online storage is often referred to as "hot storage") and/or offline (offline storage is commonly referred to as "cold storage").[28]

Figure 1: How a blockchain works



Source: "Technology: Banks seeks the key to blockchain", by J. Wild, M. Arnold and P. Stafford, 1 November 2015, Financial Times, https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64?segid=0100320#axzz3qK4rCVQP.

c. Bye-bye middleman?

One of the key advantages of blockchain technology is that it allows to simplify the execution of a wide array of transactions that would normally require the intermediation of a third party (e.g. a custodian, a bank, a securities settlement system, broker-dealers, a trade repository, …). In essence, blockchain is all about decentralizing trust and enabling decentralized authentication of transactions.[29] Simply put, it allows to cut out the "middleman".[30]

In many cases this will likely lead to efficiency gains. However, it is important to underscore that it may also expose interacting parties to certain risks that were previously managed by these

---

27 *Ibid.*, 8-9.

28 *Inter alia*: ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8; FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 8.

29 P. WITZIG and V. SALOMON, "Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry", Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf, 5.

30 It should be noted that on permissioned blockchains there is still a role for a central party (see also above).

intermediaries. For instance, the Bank for International Settlements ("***BIS***") recently warned in a report of 2017 titled *Distributed ledger technology in payment, clearing and settlement*[31], that the adoption of blockchain technology could introduce new liquidity risks.[32] More in general it seems that when an intermediary functions as a buffer against important risks, such as systemic risk, he cannot simply be replaced by blockchain technology.

2.1.3. The blockchain consensus mechanisms

In principle, any node within a blockchain network can propose the addition of new information to the blockchain. In order to validate whether this addition of information (for example a transaction record) is legitimate, the nodes have to reach some form of agreement. Here a "consensus mechanism" comes into play. In short, a consensus mechanism is a predefined specific (cryptographic) validation method that ensures a correct sequencing of transactions on the blockchain.[33] In the case of cryptocurrencies, such sequencing is required to address the issue of "double-spending" (i.e. the issue that one and the same payment instrument or asset can be transferred more than once if transfers are not registered and controlled centrally[34]).

A consensus mechanism can be structured in a number of ways. Hereinafter, the two best-known – and in the context of cryptocurrencies also most commonly used – examples of consensus mechanisms will be briefly discussed: the Proof of Work ("***PoW***") mechanism and the Proof of Stake ("***PoS***") mechanism.

a. Proof of Work (PoW)

In a PoW system, network participants have to solve so-called "cryptographic puzzles" to be allowed to add new "blocks" to the blockchain. This puzzle-solving process is commonly referred to as "mining".[35] In simple terms, these cryptographic puzzles are made up out of all information previously recorded on the blockchain and a new set of transactions to be added to the next "block".[36] Because the input of each puzzle becomes larger over time (resulting in a more complex calculation), the PoW mechanism requires a vast amount of computing resources, which consume a significant amount of electricity.[37]

---

31 CPMI, "Distributed ledger technology in payment, clearing and settlement – An analytical framework", February 2017, https://www.bis.org/cpmi/publ/d157.pdf.

32 *Ibid.*, 19.

33 See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 6.

34 R. HOUBEN, "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 195.

35 See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 6.

36 EY, "IFRS – Accounting for crypto-assets", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 17.

37 For example, the current estimated annual electricity consumption of Bitcoin (one of the best-known examples of a cryptocurrency based on a PoW mechanism) is equivalent to the annual electricity consumed in the Czech Republic. *Inter alia:* https://digiconomist.net/bitcoin-energy-consumption; S. LEE, "Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That", April 2018, https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/.

If a network participant (i.e. a node) solves a cryptographic puzzle, it proves that he has completed the work, and is rewarded with digital form of value (or in the case of a cryptocurrency, with a newly mined coin). This reward serves as an incentive to uphold the network.[38]

The cryptocurrency Bitcoin is based on a PoW consensus mechanism. Other examples include Litecoin, Bitcoin Cash, Monero, etc.[39]

b. Proof of Stake (PoS)

In a PoS system, a transaction validator (i.e. a network node) must prove ownership of a certain asset (or in the case of cryptocurrencies, a certain amount of coins) in order to participate in the validation of transactions. This act of validating transactions is called "forging"[40] instead of "mining". For example, in the case of cryptocurrencies, a transaction validator will have to prove his "stake" (i.e. his share) of all coins in existence to be allowed to validate a transaction. Depending on how many coins he holds, he will have a higher chance of being the one to validate the next block (i.e. this all has to do with the fact that he has greater seniority within the network earning him a more trusted position).[41] The transaction validator is paid a transaction fee for his validation services by the transacting parties.[42]

Cryptocurrencies such as Neo and Ada (Cardano) utilize a PoS consensus mechanism[43].

c. Other mechanisms

The PoW and PoS mechanisms are far from the only consensus mechanisms currently in existence.[44] Other examples include proof of service, proof of elapsed time and proof of capacity. A further analysis of these mechanisms falls outside the scope of this study.

2.1.4. Blockchain technology can have many applications

While blockchain technology is often associated with digital or virtual currency schemes, payments and financial services, its scope is much wider. Blockchain can theoretically be applied in a large variety of sectors[45] (e.g. trade and commerce, healthcare, governance, …). In addition, it has numerous potential applications. It could have an impact on the pledging of collateral, on the registration of shares, bonds and other assets[46], on the transfer of property tiles, on the operation of land registers[47], etc. An analysis of these applications falls outside the scope of this study.

---

38 World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 6

39 Also see below under 3.2. Bitcoin and beyond: the 10 cryptocurrencies with the highest market capitalisation.

40 One node "forges" each block. See: EY, "IFRS – Accounting for crypto-assets", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 17.

41 EY, "IFRS – Accounting for crypto-assets", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 17.

42 In principle, cryptocurrencies that utilise a PoS mechanism are already pre-mined. Hence, forging does not create new coins. See: *ibid.*

43 It should be noted that the cryptocurrency Ethereum is a special case. Ethereum has been based on a PoW mechanism from the start, but its community of developers is now planning on updating that mechanism and overlaying it with a PoS mechanism. See for example: S. JAGATI, "Ethereum's Proof of Stake Protocol Under Review", April 2018, https://cryptoslate.com/ethereums-proof-of-stake-protocol-in-review/. Also see below under 3.2.9. NEO (NEO) and 2.2.7. Cardano (ADA).

44 See also: *Ibid.*

45 See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 21.

46 CPMI, "Digital currencies", November 2015, https://www.bis.org/cpmi/publ/d137.pdf, 15.

47 See for example: W. HOLDEN, "Bringing Blockchain to Land Registry", January 2018, https://www.blockchain-expo.com/2018/01/blockchain/bringing-blockchain-land-registry/.

As pointed out above, this study will only touch upon the subject of blockchain technology where this is meaningful for the research on cryptocurrencies and can be deemed relevant from the perspective of combating money laundering, terrorist financing and/or tax evasion.

2.2. What are cryptocurrencies?

2.2.1. Introduction

Establishing a definition of cryptocurrencies is no easy task. Much like blockchain, cryptocurrencies has become a "buzzword" to refer to a wide array of technological developments that utilise a technique better known as cryptography. In simple terms, cryptography is the technique of protecting information by transforming it (i.e. encrypting it) into an unreadable format that can only be deciphered (or decrypted) by someone who possesses a secret key.[48] Cryptocurrencies such as Bitcoin, are secured via this technique using an ingenious system of public and private digital keys.[49]

Hereinafter we try to give a suitable definition of cryptocurrencies on the basis of a critical analysis of the definitions already developed by various concerned policy makers at European and international level.[50]

2.2.2. The policy makers: ECB, IMF, BIS, EBA, ESMA, World Bank and FATF

Since the emergence of Bitcoin in 2009[51], the subject of cryptocurrencies has been scrutinized by various policy makers, whom have each touched upon the subject in a different way.

a. ECB

The European Central Bank ("***ECB***") has classified cryptocurrencies as a subset of *virtual currencies*. In a report on *Virtual Currency Schemes* of 2012, it defined such currencies as a form of unregulated digital money, usually issued and controlled by its developers, and used and accepted among the members of a specific virtual community.[52]

It further clarified that three types of virtual currencies can be distinguished depending on the interaction with traditional currencies and the real economy:

i. virtual currencies that can only be used in a closed virtual system, usually in online games (e.g. *World of Warcraft Gold*);

ii. virtual currencies that are unilaterally linked to the real economy: a conversion rate exists to purchase the currency (with traditional money) and the purchased currency can subsequently be used to buy virtual goods and services (and exceptionally also to buy real goods and services) (e.g. *Facebook Credits*);

iii. virtual currencies that are bilaterally linked to the real economy: there are conversion rates both for purchasing virtual currency as for selling such currency; the purchased currency can be used to buy both virtual as real goods and services.[53]

---

48 See for example: J. Faulkner, *Getting started with Cryptography in .NET*, Mu nchen BookRix, 2016, 6.

49 R. HOUBEN, "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 195. Also see above under 2.1.2. How a blockchain works: the basics.

50 Hence, we do not explore definitions used at national level.

51 *Inter alia*: https://bitcoin.org/en/faq#who-created-bitcoin; G. HILEMAN and M. RAUCHS, "Global Cryptocurrency Benchmarking Study", Cambridge Centre for Alternative Finance, 2017, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, 15.

52 ECB, "Virtual Currency Schemes", October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 13.

53 *Ibid.*, 13-19.

Cryptocurrencies, such as Bitcoin, are virtual currencies of the latter type: they can both be bought with traditional money as sold against traditional money, and they can be used to buy both digital and real goods and services.[54]

In a more recent report of 2015 titled *Virtual Currency Schemes – a further analysis*, the ECB put forward a "second", and largely updated, definition of virtual currencies. It defined virtual currencies as digital representations of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money.[55] It also clarified that cryptocurrencies, such as Bitcoin, constitute a decentralized bi-directional (i.e. bilateral) virtual currency.[56]

b. IMF

Like the ECB, the International Monetary Fund ("***IMF***") has categorised cryptocurrencies as a subset of *virtual currencies*, which it defines as digital representations of value, issued by private developers and denominated in their own unit of account.[57] According to the IMF, the concept of virtual currencies covers a wider array of 'currencies', ranging from simple IOUs ("Informal certificates of debt" or "I owe you's") by issuers (such as Internet or mobile coupons and airline miles), virtual currencies backed by assets such as gold, and cryptocurrencies such as Bitcoin.[58]

c. BIS

The Committee on Payments and Market Infrastructures (*"**CPMI**"*), a body of the Bank for International Settlements ("***BIS***"), has qualified cryptocurrencies as *digital currencies* or *digital currency schemes*.[59] These schemes are said to exhibit the following key features:

i. they are assets, the value of which is determined by supply and demand, similar in concept to commodities such as gold, yet with zero intrinsic value;

ii. they make use of distributed ledgers to allow remote peer-to-peer exchanges of electronic value in the absence of trust between parties and without the need for intermediaries; and

iii. they are not operated by any specific individual or institution.[60]

d. EBA

The European Banking Authority ("***EBA***") has suggested to refer to cryptocurrencies as *virtual currencies*, which it defines[61] as digital representations of value that are neither issued by a central

---

54 *Inter alia*: BANQUE DE FRANCE, "Les dangers liés au développement des monnaies virtuelles: l'exemple de bitcoin", in Focus, no. 10, 5 December 2013, https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus-10-stabilite-financiere.pdf, 2; R. HOUBEN, "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 194; N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 75-76.

55 ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 4.

56 *Ibid.*, 9.

57 IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 7.

58 *Ibid.*

59 CPMI, "Digital currencies", November 2015, https://www.bis.org/cpmi/publ/d137.pdf, footnote 2: "*this report uses the term "digital currencies", because, while recognising that the term is not perfect, the term is used widely and reflects the concept that these are assets that are represented in digital form. Previous CPMI reports used the term "virtual currencies", reflecting their existence in a virtual rather than physical form; virtual currencies in particular are prevalent in certain online environments. Moreover, these schemes are frequently referred to as "cryptocurrencies", reflecting the use of cryptography in their issuance, and in the validation of transactions*".

60 *Ibid.*, 4-7.

61 It should be noted that EBA has indicated that the usage of the term 'currency' may be misleading in some cases. It has however opted to use this term due to its common public usage at the time (i.e. 2014). See: EBA, "EBA Opinion on 'virtual currencies'", 4 July 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf, 11.

bank or public authority nor necessarily attached to a fiat currency but are used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.[62]

e. ESMA

The European Securities and Markets Authority ("***ESMA***") has recently also referred to cryptocurrencies as *virtual currencies*, in a pan-European warning issued in cooperation with the European Insurance and Occupational Pensions Authority ("***EIOPA***") and the EBA.[63] Fully in line with the EBA's definition, virtual currencies are defined as digital representations of value that are neither issued nor guaranteed by a central bank or public authority and do not have the legal status of currency or money.[64]

f. World Bank

The World Bank has classified cryptocurrencies as a subset of *digital currencies*, which it defines as digital representations of value that are denominated in their own unit of account, distinct from e-money, which is simply a digital payment mechanism, representing and denominated in fiat money.[65]

Contrary to most other policy makers, the World Bank has also defined cryptocurrencies itself as digital currencies that rely on cryptographic techniques to achieve consensus.[66]

g. FATF

Like many other policy makers, the Financial Action Task Force ("***FATF***") has approached cryptocurrencies as a subset of *virtual currencies*, which it defines as digital representations of value that can be digitally traded and function as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but do not have legal tender status (i.e., when tendered to a creditor, are a valid and legal offer of payment) in any jurisdiction.[67]

It further suggests that virtual currencies can be divided into two basic types:

i. convertible virtual currencies that have an equivalent value in real currency and can be exchanged back-and-forth for real currency; these virtual currencies can be of a centralised or a decentralized nature (i.e. they can either have a central administrating authority that controls the system or no central oversight at all); and

ii. non-convertible virtual currencies that are specific to a particular virtual domain or world (e.g. a Massively Multiplayer Online Role-Playing Game like *World of Warcraft*), and under the rules governing its use, cannot be exchanged for fiat currency.[68]

---

62 *Ibid*. See also: Speech by Andrea Enria, Chairperson of EBA, "Designing a Regulatory and Supervisory Roadmap for FinTech", 9 March 2018, http://www.eba.europa.eu/documents/10180/2151635/Andrea+Enria%27s+speech+on+FinTech+at+Copenhagen+Business+School+090318.pdf, 5.

63 See: ESMA, EBA & EIOPA, "Warning on the risks of Virtual Currencies https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf, 1.

64 *Ibid.*

65 See: World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, IV.

66 *Ibid.*

67 FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 4.

68 *Ibid.*, 4-5.

Cryptocurrencies like Bitcoin are virtual currencies of the first type, that can, according to the FATF, be defined as math-based, decentralized convertible virtual currencies that are protected by cryptography.[69]

h. Summary

The main conclusion that can be drawn from the different perspectives set out above, is that there is no generally accepted definition of the term *cryptocurrencies* available in the regulatory space. Even more, most policy makers have refrained from defining the term altogether. Amongst those cited above, only the World Bank and the FATF have put forward a clear-cut definition. It is clear, however, that most policy makers approach cryptocurrencies as a subset or a form of virtual or digital currencies.

If we try to summarize all the above definitions, a good summary could be that a cryptocurrency is "*a digital representation of value that (i) is intended to constitute a peer-to-peer ("P2P") alternative to government-issued legal tender, (ii) is used as a general-purpose medium of exchange (independent of any central bank), (iii) is secured by a mechanism known as cryptography and (iv) can be converted into legal tender and vice versa*".

Hereinafter we will shed some light on the concept of cryptocurrencies (or coins; we will use both terms interchangeably hereinafter), more in particular the dividing line with other, neighboring concepts, which should nevertheless be distinguished from cryptocurrencies.

2.2.3. Cryptocurrencies – Tokens – Cryptosecurities

The term cryptocurrencies is in practice often erroneously used in a very broad sense.[70] As will be shown below, it should be distinguished from both tokens and cryptosecurities.

a. Cryptocurrencies – Tokens

Firstly, cryptocurrencies should be distinguished from cryptographic "tokens", which offer a functionality other than and beyond that of a general-purpose medium of exchange. Tokens are issued in the framework of an Initial Token Offering or "ITO"[71] to raise funds for a given project or enterprise. They constitute a novel class of crypto-assets (i.e. digital assets recorded on a distributed ledger, secured by cryptography[72]) which embody some sort of claim against an entity (or against its cash flows, assets, residual value, future goods or services, …) that arises from the use of blockchain technology.[73]

Some tokens resemble traditional instruments such as shares or bonds and are commonly referred to as "security tokens" or "investment tokens".[74] Other tokens grant their holders (future) access to

---

69 *Ibid.*, 5.

70 In some cases, the term "Cryptocurrency" could even be called a misnomer. See: A. ZAINUDDIN, "Differences Between Cryptocurrency Coins and Tokens", 2017, https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/.

71 We note that legal literature and popular media commonly refer to these fundraising events as Initial Coin Offerings or ICOs (see for example: J. ROHR and A. WRIGHT, "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets", October 2017 (electronically available via https://ssrn.com/abstract=3048104); D. ZETZSCHE, R. P. BUCKLEY, D. W. ARNER and L. FÖHR, "The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators", November 2017 (electronically available via https://ssrn.com/abstract=3072298); D. FLOYD, "$6.3 Billion: 2018 ICO Funding Has Passed 2017's Total", April 2018, https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/). If we take the position that tokens actually differ from coins, then the term Initial Token Offering or ITO is a more appropriate term for future reference.

72 EY, "IFRS – Accounting for crypto-assets", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 2.

73 See: A. SNYERS and K. PAUWELS, "ICOs in Belgium: down the rabbit hole into legal no man's land? (Part 1)", ICCLR, 2018, to be published.

74 *Ibid.*

specific products or services and are commonly referred to as "utility tokens". They can be used to acquire certain products or services, yet they do not constitute a general-purpose medium of exchange, simply because they can generally only be used on the token platform itself.[75]

b. Cryptocurrencies – Cryptosecurities

Secondly, cryptocurrencies should also be distinguished from a concept that has recently been referred to as "cryptosecurities".[76] In short, it has been argued that blockchain technology could also be used to register, issue and transfer regular shares and other corporate securities, so that the capitalisation table of a company is always accurate and up-to-date.[77] Because this technological process would be secured with cryptography, it has been suggested that these securities be defined as cryptosecurities.

The only connection between this newly developed concept "cryptosecurities" and cryptocurrencies, is that they both utilize blockchain technology.

2.2.4. Cryptocurrencies – Blockchain

Cryptocurrencies and blockchain have become hot topics in the last couple of years. Whilst the two are often referred to in the same sentence and are clearly linked to each other, one should never mistake one for the other. Blockchain is a type of distributed ledger technology that forms the backbone of the crypto-market. It is the technology behind the large variety of cryptocurrencies currently in circulation. Its scope and field of application are, however, not limited thereto. As set out above, blockchain can be applied in various sectors and can have a wide array of applications. It is important to draw a clear line between these applications and cryptocurrencies, which are but one specific application of blockchain technology. Against this background, regulators need not fear of stifling innovation when tackling the subject of cryptocurrencies.

2.3. Who are the players involved?

The cryptocurrency market is a new playing field where different actors each play a particular role. To shed some more light on how the market works, and without attempting to be exhaustive, we will hereinafter further identify the key players.

---

[75] It should be noted that various studies of the token market have put forward taxonomies of tokens. Not all of these taxonomies coincide, yet the silver thread that appears to run through all of them is that, at the very least, a distinction is to be made between "security" or "investment tokens" on the one hand and "utility tokens" on the other hand. See *inter alia*: D. ZETZSCHE, R. P. BUCKLEY, D. W. ARNER and L. FÖHR, "The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators", November 2017 (electronically available via https://ssrn.com/abstract=3072298); J. ROHR and A. WRIGHT, "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets", October 2017, (electronically available via https://ssrn.com/abstract=3048104); EY, "Research: initial coin offerings (ICOs)", December 2017, http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf; Laga, "Initial Coin Offerings - Legal qualification and regulatory challenges", March 2018, https://www.slideshare.net/fintechbelgium/fintech-belgium-meetup-on-icos-080318-laurent-godts; FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", February 2018, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en; P. HACKER and C. THOMALE, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", November 2017 (electronically available via https://ssrn.com/abstract=3075820); A. SNYERS and K. PAUWELS, "ICOs in Belgium: down the rabbit hole into legal no man's land? (Part 1)", ICCLR, 2018, to be published.

[76] M. VAN DE LOOVERBOSCH, "Crypto-effecten: tussen droom en daad", TRV-RPS 2018, 193-207.

[77] *Ibid.*, 198, nº 22-23. See also: P. PAECH, "Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty", LSE Law, Society and Economy Working Paper 20/2015, 26-28. It should be noted that while blockchain technology is currently not yet being widely applied in the context of corporate law, it already has some legal applications (i.e. in the US (Delaware) and France). See for France: Ordonnance n° 2017-1674 du 8 de cembre 2017 relative a l'utilisation d'un dispositif d'enregistrement e lectronique partage pour la repre sentation et la transmission de titres financiers, JORF 9 december 2017, nº 0287, text nº 24, www.legifrance.gouv.fr/eli/ordonnance/2017/12/8/2017-1674/jo/texte; see for Delaware: Delaware General Assembly, Senate Bill 69, https://legis.delaware.gov/BillDetail?legislationId=25730; D. LUCKING and C. O'HANLON, "Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares", 26 September 2017, http://www.allenovery.com/publications/en-gb/Pages/Delaware-Passes-Law-Permitting-Companies-to-Use-Blockchain-Technology-to-Issue-and-Track-Shares-.aspx.

2.3.1. Cryptocurrency users

A first, and very important, player is the "**cryptocurrency user**". A cryptocurrency user is a natural person or legal entity who obtains coins to use them (i) to purchase real or virtual goods or services (from a set of specific merchants[78]), (ii) to make P2P payments, or (iii) to hold them for investment purposes (i.e. in a speculative manner).[79]

Without trying to be exhaustive, a cryptocurrency user can obtain his coins in a number of ways[80]:

- Firstly, he can simply buy his coins on a cryptocurrency exchange using fiat money or another cryptocurrency;
- Secondly, he can buy his coins directly from another cryptocurrency user (i.e. through a trading platform – this form of exchange is often referred to as a "P2P exchange");
- Thirdly, if a cryptocurrency is based on a PoW consensus mechanism, he can mine a new coin (i.e. participate in the validation of transactions by solving of a "cryptographic puzzle" and be rewarded a new coin[81]);
- Fourthly, in some cases he can obtain his coins directly from the coin offeror, either as part of a free initial offering of coins (e.g. on the Stellar network Lumens (XLM) are being given away for free[82]) or in the framework of a crowd sale set-up by the coin offeror (e.g. a large bulk of ether (*cf.* Ethereum) was sold in a crowdsale to cover certain development costs[83]);
- Fifthly, if he sells goods or services in exchange for cryptocurrency, he can also receive coins as a payment for those goods or services;
- Sixthly, in case of a "hard fork"[84] of a coin's blockchain, he will automatically obtain an amount of the newly created coin; and
- Finally, he can receive coins as a gift or donation from another cryptocurrency user.

2.3.2. Miners

A second player is the "**miner**" who participates in validating transactions on the blockchain by solving a "cryptographic puzzle". As explained above, the process of mining relates to cryptocurrencies that are based on a PoW consensus mechanism. A miner supports the network by harnessing computing power to validate transactions and is rewarded with newly mined coins (i.e. through an automatic decentralized new issuance).[85] Miners can be cryptocurrency users, or, more commonly, parties who have made a new business out of mining coins to sell them for fiat currency

---

78 At present, only a limited number of (online) merchants accepts payments in Cryptocurrencies. See for example for the Cryptocurrency Litecoin: https://litecoin.com/services#merchants.

79 See *inter alia*: FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 7; ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8; COMMISSION STAFF WORKING DOCUMENT Accompanying the document "Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations", COM(2017) 340 final, Annex, Part 2, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF, 85.

80 See also: ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8.

81 Also see above under 2.1.3. The blockchain consensus mechanisms.

82 See: https://www.stellar.org/lumens/. Also see below under 3.2.6. Stellar (XLM).

83 Also see below under 3.2.2. Ethereum (ETH).

84 This concept is discussed and explained further below under "Bitcoin Cash".

85 ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 7.

(such as US dollar or Euro) or for other cryptocurrencies.[86] Some miners group in so-called pools of miners to bundle computing power.[87]

At present, the risks associated with so-called "mining businesses" appear to be underestimated. We will further elaborate on this below.[88]

2.3.3. Cryptocurrency exchanges

A third group of key players are the so-called "**cryptocurrency exchanges**". Cryptocurrency exchanges are persons or entities who offer exchange services to cryptocurrency users, usually against payment of a certain fee (i.e. a commission). They allow cryptocurrency users to sell their coins for fiat currency or buy new coins with fiat currency.[89] They usually function both as a bourse and as a form of exchange office.[90] Examples of well-known cryptocurrency exchanges are: Bitfinex[91], HitBTC[92], Kraken[93] and Coinbase GDAX[94].[95]

It is important to note that some exchanges are *pure* cryptocurrency exchanges, which means that they only accept payments in other cryptocurrencies, usually Bitcoin (for example Binance[96]), whilst others also accept payments in fiat currencies such as US dollar or Euro (for example Coinbase). Furthermore, many cryptocurrency exchanges only allow their users to buy a particular selection of coins.

It should also be noted that many cryptocurrency exchanges (i.e. both regular and pure cryptocurrency exchanges) operate as custodian wallet providers[97] (for example Bitfinex).

In general cryptocurrency exchanges offer their users a wide array of payment options, such as wire transfers, PayPal transfers, credit cards and other coins.[98] Some cryptocurrency exchanges also provide statistics on the cryptocurrency market (like trading volumes and volatility of the coins traded[99]) and offer conversion services to merchants who accept payments in cryptocurrencies.

---

86 FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 7.

87 See: COMMISSION STAFF WORKING DOCUMENT Accompanying the document "Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations", COM(2017) 340 final, Annex, Part 2, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF, 85.

88 See 5.3.3 Miners.

89 FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 7.

90 *Ibid.;* It should be noted that there is currently also a very limited number of so-called Cryptocurrency ATMs (e.g. Bitcoin ATMs) on the market, which also qualify as cryptocurrency exchanges. See: COMMISSION STAFF WORKING DOCUMENT Accompanying the document "Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations", COM(2017) 340 final, Annex, Part 2, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF, 86.

91 See: https://www.bitfinex.com.

92 See: https://hitbtc.com.

93 See: https://www.kraken.com.

94 See: https://www.coinbase.com.

95 See for other examples: https://cryptocoincharts.info/markets/info.

96 See: https://www.binance.com.

97 See further below: 2.3.5 Wallet providers.

98 See: ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8.

99 For example, the Bitfinex Cryptocurrency Exchange offers a number of statistics, as well as conversion rates against fiat currency; see: https://www.bitfinex.com.

2.3.4. Trading platforms

In addition to cryptocurrency exchanges, so-called "**trading platforms**" also play an important role in the exchange of cryptocurrencies (and, most notably, allow cryptocurrency users to buy coins with cash). Trading platforms are market places that bring together different cryptocurrency users that are either looking to buy or sell coins, providing them with a platform on which they can directly trade with each other (i.e. an "eBay" for cryptocurrencies).[100]

Trading platforms are sometimes referred to as "P2P exchanges" or "decentralized exchanges".[101] They differ from cryptocurrency exchanges in a number of ways. First and foremost, they do not buy or sell coins themselves.[102] Secondly, they are not run by an entity or company that oversees and processes all trades, but they are operated exclusively by software (i.e. there is no central point of authority).[103] Trading platforms simply connect a buyer with a seller, allowing them to conduct a deal, online, or even locally in-person (i.e. a face-to-face trade, often executed in cash). A well-known example of a trading platform for Bitcoins is LocalBitcoins[104].

2.3.5. Wallet providers

Another group of key players are the so-called "**wallet providers**". Wallet providers are those entities that provide cryptocurrency users digital wallets or e-wallets which are used for holding, storing and transferring coins.[105] Simply put, a wallet holds a cryptocurrency user's cryptographic keys (see above). A wallet provider typically translates a cryptocurrency user's transaction history into an easily readable format, which looks much like a regular bank account.[106]

In reality, there are several types of wallet providers[107]:

- *Hardware wallet providers* that provide cryptocurrency users with specific hardware solutions to privately store their cryptographic keys (e.g. Ledger Wallet[108], …);
- *Software wallet providers* that provide cryptocurrency users with software applications which allow them to access the network, send and receive coins and locally save their cryptographic keys (e.g. Jaxx[109]);
- *Custodian wallet providers* that take (online) custody of a cryptocurrency user's cryptographic keys (e.g. Coinbase[110]).

---

100 ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8.

101 See: A. MARSHALL, "P2P Cryptocurrency Exchanges, Explained", April 2017, https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained.

102 ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8.

103 See: A. MARSHALL, "P2P Cryptocurrency Exchanges, Explained", April 2017, https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained.

104 See: https://localbitcoins.com.

105 FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 8.

106 See also: ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8.

107 See also: COMMISSION STAFF WORKING DOCUMENT Accompanying the document "Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations", COM(2017) 340 final, Annex, Part 2, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF, 85; T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 14 (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

108 See: https://www.ledgerwallet.com/products.

109 See: https://jaxx.io.

2.3.6. Coin inventors

There are also those players who are referred to as "**coin inventors**". Coin inventors are individuals or organizations who have developed the technical foundations of a cryptocurrency and set the initial rules for its use.[111] In some cases their identity is known (e.g. Ripple, Litecoin, Cardano), but ever so often they remain unidentified (eg. Bitcoin, Monero). Some remain involved in maintaining and improving the cryptocurrency's code and underlying algorithm (in principle without administrator's powers), whilst others simply disappear (e.g. Bitcoin).[112]

2.3.7. Coin offerors

A final group of key players to be distinguished are the "**coin offerors**". Coin offerors are individuals or organizations that offer coins to cryptocurrency users upon the coin's initial release, either against payment (i.e. through a crowdsale) or at no charge (i.e. in the framework of a specific (sign-up) program (e.g. Stellar – see below)), normally to fund the coin's further development or boost its initial popularity.

The coins these coin offerors offer to cryptocurrency users are created or pre-mined prior to the coin's official release / the coin's inception. Coins that are distributed this way are either partially pre-mined or pre-created (i.e. cryptocurrency users can still generate more coins after the release), or are fully pre-mined or pre-created. In the latter case the coin offeror usually retains a large portion of the coins (e.g. this is the case with Stellar).

It is important to note that not all coins have an identifiable coin offeror, nor are all coins pre-mined or is its full supply pre-created.

A coin offeror can be the same person as the coin inventor, or another individual or organization.

---

110 See *inter alia*: https://support.coinbase.com/customer/en/portal/topics/601112-wallet-services/articles.

111 ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 7.

112 *Ibid.*

3. CLASSIFYING CRYPTOCURRENCIES

3.1. Scoping the Crypto-Market

After having known a steady growth over the last couple of years, the market for cryptocurrencies has skyrocketed in 2017, appreciating more than 1,200%.[113] At present, there are several hundreds of coins in circulation (with a total market capitalisation of well over EUR 300 billion)[114], and more continue to pop up on a regular basis. In order to fully grasp this emerging market and carry out a meaningful study, we have opted to first analyse the key properties of the best-known cryptocurrency Bitcoin and then tackle the main features of a selected number of alternative cryptocurrencies, better known as "**Altcoins**".

Altcoins are all coins that are an alternative to Bitcoin.[115] In short, there are two types of Altcoins:

- Altcoins that are built using Bitcoin's original open-source protocol, with a number of changes to its underlying codes[116], conceiving a new coin with a different set of features.[117] An example of such an Altcoin is Litecoin.[118]
- Altcoins that are not based on Bitcoin's open-source protocol, but that have their own protocol and distributed ledger. Well-known examples of such Altcoins are Ethereum and Ripple.[119]

This study will focus on the ten Altcoins that currently have the highest market capitalisation (see Table 1).[120] We have made this selection, not only on the basis of the current popularity of these Altcoins within the "crypto-community", but also because they exhibit a wide range of different features. Some of them are based on Bitcoin's original open-source protocol, whilst others constitute an entirely new platform and/or eco-system. Some utilise a PoW mechanism, others employ another form of consensus mechanism. Most are characterised as pseudo-anonymous, yet some are said to even be fully anonymous (meaning that the amount of coins their users own, send and receive is not observable, traceable or linkable through the blockchain's transaction history[121]).

---

[113] See: C. BOVAIRD, "Why the crypto market has appreciated more than 1,200% this year", November 2017, https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#3906c8d6eed3. See for some interesting charts on the growth of the market: https://coinmarketcap.com/charts/.

[114] According to data available on https://coinmarketcap.com/coins/views/all/ (data derived on 27 May 2018) the number of Coins in circulation nears 900. If we count both Coins and Tokens, the crypto-market already exceeds a total of 1600 different crypto-assets.

[115] FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 6. See also: D. HELLER, "The implications of digital currencies for monetary policy", in-depth analysis commissioned by the Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, May 2017, 7 (electronically available via http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL_IDA(2017)602048_EN.pdf).

[116] Bitcoin's original protocol is available via https://bitcoin.org/bitcoin.pdf.

[117] ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 9. See also: A. ZAINUDDIN, "Coins, Tokens & Altcoins: What's the Difference?", 2017, https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/.

[118] See *inter alia*: J. MARTINDALE, "What is Litecoin? Here's everything you need to know", January 2018, https://www.digitaltrends.com/computing/what-is-litecoin/. See also: T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, http://digitalcommons.law.msu.edu/jbsl, 163.

[119] See: A. ZAINUDDIN, "Coins, Tokens & Altcoins: What's the Difference?", 2017, https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/.

[120] This selection was made on 27 May 2018 at 15:00 PM, on the basis of data derived from https://coinmarketcap.com/coins/views/all/.

[121] See *inter alia*: A. ZAINUDDIN, "Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies", 2017, https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/; P. GLAZER, "An Overview of Privacy Coins", February 2018, https://hackernoon.com/an-overview-of-privacy-tokens-19f6af8077b7; L. NEL, "Privacy Coins: Beginner's Guide to Anonymous Cryptocurrencies", April 2018, https://blockonomi.com/privacy-cryptocurrency/. Also see below under 3.2.10. Monero (XMR) and 3.2.11. Dash (DASH).

The below analysis of the selected cryptocurrencies is based solely on the information available to the public via the internet.

Table 1: Overview of coins

Name	Symbol		Market Cap[122]	Supply limit[123]
Bitcoin		BTC	$124.969.093.161	21 million
Ethereum		ETH	$57.462.517.858	TBD[124]
Ripple		XRP	$23.790.387.789	100 billion
Bitcoin Cash		BCH	$17.159.025.225	21 million
Litecoin		LTC	$6.704.709.572	84 million
Stellar		XLM	$5.128.373.973	100 billion
Cardano		ADA	$5.034.129.651	45 billion
IOTA		MIOTA	$4.038.240.572	2,779,530,283,277,761
NEO		NEO	$3.386.383.000	100 million
Monero		XMR	$2.626.586.260	18,4 million
Dash		DASH	$2.592.894.544	17.74 – 18.92 million[125]

[122] This data has been derived from https://coinmarketcap.com/coins/views/all/ on 27 May 2018 at 15:00 PM. It should be noted that this data is very volatile, like the cryptocurrency market itself. For purposes of convencience we have opted to present this data in its original form, i.e. denominated in US dollar.

[123] This data has been derived from different websites set-up and supported by members of each respective cyrptocurrency community. See: https://bitcoin.org (BTC); https://www.ethereum.org (ETH); https://ripple.com (XRP); https://www.bitcoincash.org (BCH); https://litecoin.com (LTC); https://www.stellar.org (XLM); https://www.cardano.org (ADA); https://www.iota.org (MIOTA); https://neo.org (NEO); http://www.monero.cc (XMR); https://www.dash.org (DASH).

[124] We note that Ethereum's co-inventor Vitalik Buterin recently launched a proposal in the Ethereum community to limit the total supply of ETH to 120,204,432. See: L. K. ABIOLA, 'Ethereum (ETH) Co-Founder Provides Answer To Long-Lived Supply Limit Question', April 2018, https://oracletimes.com/ethereum-eth-co-founder-provides-answer-to-long-lived-supply-limit-question/; K. SHAH, 'Ethereum Supply Limit to 120 million – Prank or Reality?', April 2018, https://www.cryptoground.com/a/ethereum-supply-limit-to-120-million.

[125] The total supply limit of Dash depends on the allocation of block rewards, which in turn depends on future voting behaviour within the Dash network. See: https://docs.dash.org/en/latest/introduction/features.html.

3.2. Bitcoin and beyond: the 10 cryptocurrencies with the highest market capitalisation

3.2.1. Bitcoin (BTC)

a. What is Bitcoin?

Bitcoin (BTC) is usually described as a virtual, decentralized and (at first glance) anonymous currency that is not government-backed or backed by any other legal entity, and that can not be exchanged into gold or any other commodity.[126]

At the heart of the creation of Bitcoin stands the text "*Bitcoin: a Peer-to-Peer Electronic Cash System*" of Satoshi Nakamoto[127], published on the internet in 2008. It was on the basis of this text and the ideas conveyed in it that the development of Bitcoin accelerated. Contributory to the mystic nature of Bitcoin is that until now it remains unclear whether Satoshi Nakamoto is a real person, a pseudonym, or perhaps even a group of hackers.[128]

The virtual character of Bitcoin implies that Bitcoins normally do not take a physical form. Therefore, a good representation of a Bitcoin probably is that of a computer file saved on a personal computer or, via an online service, in a digital wallet.[129] The mere virtual character of Bitcoins should, however, be qualified. Reputedly, it is possible to print out the combination of characters that constitute the

---

[126] R. GRINBERG, "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal, 2011, Vol. 4, 160 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857). Also see the similar, yet sometimes gradually differing definitions set forth in: N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 2 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203); J. BRITO, H. SHADAB and A. CASTILLO, "Bitcoin financial regulation: securities, derivatives, prediction markets & gambling", 24 July 2014, 4 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423461); L.J. TRAUTMAN, "Virtual currencies: Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?", Richmond Journal of Law and Technology, Vol. 20, No. 4, 2014, 5 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393537); D. BRYANS, "Bitcoin and Money Laundering: Mining for and Effective Solution" Indiana Law Journal, 2014, Vol. 89: Iss. 1, Article 13, 443 (electronically available via https://www.repository.law.indiana.edu/ilj/vol89/iss1/13); R. BOLLEN, "The Legal Status of Online Currencies: Are Bitcoins the Future?", Journal of Banking and Finance Law and Practice 2013, 3 (electronically available via http://ssrn.com:80/abstract=2285247); N.A. PLASSARAS, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", Chicago Journal of International Law, 2013, 4 (electronically available http://ssrn.com:80/abstract=2248419); LAM PAK NIAN, "Bitcoin in Singapore: A Light-Touch Approach to Regulation", 11 April 2014, 9 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427626); B.E GUP, "What Is Money? From Commodities to Virtual Currencies/Bitcoin" (14 March 2014), 6 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172). Also see the influential publication of the ECB: ECB, "Virtual Currency Schemes", October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 21. R. HOUBEN, "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 193-208.

[127] Which can be found via https://bitcoin.org/bitcoin.pdf. Satoshi Nakamoto in turn was inspired by the ideas of W. Dai, as set out in a text of 1998 titled "b-money" (electronically available via: http://www.weidai.com/bmoney.txt). See on the history of Bitcoin: R. GRINBERG, "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal, 2011, Vol. 4, 162 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857); ECB, "Virtual Currency Schemes", October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 21; D. BRYANS, "Bitcoin and Money Laundering: Mining for and Effective Solution" Indiana Law Journal, 2014, Vol. 89: Iss. 1, Article 13, 444 (electronically available via https://www.repository.law.indiana.edu/ilj/vol89/iss1/13); N.A. PLASSARAS, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", Chicago Journal of International Law, 2013, 13-14 (electronically available http://ssrn.com:80/abstract=2248419).

[128] See the recent speculations made by L. MCGRATH GOODMAN, "The Face Behind Bitcoin", in Newsweek, 14 March 2014, http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html.

[129] *Inter alia*: N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 4 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203); N.A. PLASSARAS, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", Chicago Journal of International Law, 2013, 6 (electronically available http://ssrn.com:80/abstract=2248419). We reiterate that such wallets are normally not offered by credit institutions or investment institutions, but by non-regulated entities (i.e. so-called wallet providers). For that reason alone depositors of Bitcoins are not protected by deposit guarantee schemes or investor compensation schemes, as these schemes only apply to deposits at credit institutions and/or investment entities (*cf.* Directive 94/19/EC of 30 May 1994 *on deposit guarantee schemes, OJ L* 31 May 1994, iss. 135, p. 5 and Article 380 of the Belgian Act of 25 April 2014 *on the legal status and supervision of credit institutions* and Directive 97/9/EC of 3 March 1997 *on investor compensation schemes, OJ L* 26 March 1997, iss. 84, p. 22).

Bitcoin and, subsequently, to transfer such print as a bearer instrument[130]. However, this is supposed to be a marginal phenomenon and, hence, will not further elaborated here.

Bitcoin is based on a PoW consensus mechanism. The issue of Bitcoins takes place via a process called "*mining*" (see also above). To reiterate, such process the entire elements of which are publicly available via open-source software – entails that persons voluntarily make their own computers available to the Bitcoin network to solve complex mathematical problems.[131] Computers that are able to solve such problems (and, as a consequence, are able to create so-called transaction "*blocks*") are rewarded with Bitcoins.[132]

The aggregate number of Bitcoins that can be created through mining is limited: the Bitcoin system is programmed so that the development of blocks in time will be rewarded with increasingly less Bitcoins and that at no point in time will more than 21 million Bitcoins exist.[133] The fact that the creation and the increase of Bitcoins is automated and limited by the system itself implies that there is no need for the intervention of a central entity / authority to issue Bitcoins.[134]

The limited number of Bitcoins, together with the fact that conversion rates for Bitcoins are determined by supply and demand, without a government body being able to intervene (e.g. by printing additional money), results in a high volatility in Bitcoins prices.[135]

b. Bitcoin runs on an open, permissionless blockchain

The Bitcoin blockchain is a typical example of an open, permissionless blockchain.[136] Any person can join or leave the public Bitcoin network at will, without having to be (pre-)approved by any (central) entity. All that is needed to join the Bitcoin network and add transactions to the ledger is a computer on which the relevant software has been installed.

---

130 EBA, "EBA Opinion on 'virtual currencies'", 4 July 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf, 12.

131 N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 7 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203); ECB, "Virtual Currency Schemes", October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 21 and 24.

132 N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 7 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203).

133 N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 8 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203); R. BOLLEN, "The Legal Status of Online Currencies: Are Bitcoins the Future?", Journal of Banking and Finance Law and Practice 2013, 6 (electronically available via http://ssrn.com:80/abstract=2285247), R. GRINBERG, "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal, 2011, Vol. 4, 163 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857); ECB, "Virtual Currency Schemes", October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 25; D. BRYANS, "Bitcoin and Money Laundering: Mining for and Effective Solution" Indiana Law Journal, 2014, Vol. 89: Iss. 1, Article 13, 446-447 (electronically available via https://www.repository.law.indiana.edu/ilj/vol89/iss1/13); N.A. PLASSARAS, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", Chicago Journal of International Law, 2013, 8 (electronically available http://ssrn.com:80/abstract=2248419).

134 N.M. KAPLANOV, "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 8 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203).

135 Also see the press release of the NBB and the FSMA of 14 January 2014 (http://www.fsma.be/nl-in-the-picture/Article/press/div/2014/2014-01-14_virtueel.aspx) and in BANQUE DE FRANCE, "Les dangers liés au développement des monnaies virtuelles: l'exemple de bitcoin", in Focus, no. 10, 5 December 2013, https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus-10-stabilite-financiere.pdf, 4; R. BOLLEN, "The Legal Status of Online Currencies: Are Bitcoins the Future?", Journal of Banking and Finance Law and Practice 2013, 4 (electronically available via http://ssrn.com:80/abstract=2285247); B.E GUP, "What Is Money? From Commodities to Virtual Currencies/Bitcoin" (14 March 2014), 7 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172); J. BRITO, H. SHADAB and A. CASTILLO, "Bitcoin financial regulation: securities, derivatives, prediction markets & gambling", 24 July 2014, 11-14 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423461).

136 See for example: R. LEWIS, J. MCPARTLAND and R. RANJAN, "Blockchain and financial market innovation", Economic Perspectives, Issue 7, 2017, Federal Reserve Bank of Chicago (electronically available via https://www.chicagofed.org/publications/economic-perspectives/2017/7).

c. Bitcoin is directly convertible into fiat currency

Bitcoin can be bought with and directly converted into fiat currency on a wide array of cryptocurrency exchanges (e.g. Coinbase, Kraken, Anycoin Direct[137], Lunco[138], …). Out of all cryptocurrencies currently in circulation, Bitcoin is one of the easiest coins to convert into fiat currency.

d. Bitcoin is a medium of exchange

Bitcoin (BTC) is being accepted as a legitimate source of funds by a relatively large number of (online) merchants, among which various large companies (e.g. Microsoft[139], Expedia[140], Playboy[141], Virgin Galactic[142], LOT Polish Airlines[143], ….)[144]. As a result it can be qualified as a medium of exchange.

e. Bitcoin is a pseudo-anonymous coin

Bitcoin is often characterized as an *anonymous* currency: although everyone can verify the chain of transactions on the basis of the public ledger, at first glance nothing in the system connects Bitcoins to individuals.[145] However, this anonymous character is far from absolute. It is technically feasible – though very complex and costly – to identify the parties behind a Bitcoin transaction by bringing together factors that accompany such transaction.[146] In other words, Bitcoin is not a fully anonymous currency, but rather a pseudo-anonymous coin.[147]

3.2.2. Ethereum (ETH)

a. What is Ethereum?

Ethereum, launched in July 2015[148], is a decentralized platform that runs so-called "smart contracts". Smart contracts are "self-executing" contracts or applications that run exactly as programmed without any possibility of downtime (i.e. the blockchain is never down, it is always running), censorship, fraud or third-party interference.[149]

---

137 See: https://anycoindirect.eu/.

138 See: https://www.luno.com.

139 Microsoft accepts payments with Bitcoin in its Xbox online store for games and movies. See: https://support.microsoft.com/nl-be/help/13942/microsoft-account-add-money-with-bitcoin.

140 See: https://www.expedia.com/Checkout/BitcoinTermsAndConditions.

141 See: http://fortune.com/2018/03/14/playboy-cryptocurrency-vice-vit-crypto/.

142 See: https://www.virgin.com/richard-branson/bitcoins-space.

143 See: https://www.coindesk.com/lot-polish-airlines-accept-bitcoin/.

144 See for more examples: https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/.

145 R. GRINBERG, "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal, 2011, Vol. 4, 164 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857); ECB, "Virtual Currency Schemes", October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 23.

146 M. FLEDER, M.S. KESTER and S. PILAI, "Bitcoin Transaction Graph Analysis", January 2014 (electronically available via http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf): "In conclusion, we showed that by leveraging several sources of publicly available information via web-scraped forums and Bitcoin's transaction ledger, the Bitcoin transaction network is shown to be not entirely anonymous.". Also see LAM PAK NIAN, "Bitcoin in Singapore: A Light-Touch Approach to Regulation", 11 April 2014, 14-15 (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427626).

147 See: A. VAN WIRDUM, "Is Bitcoin Anonymous? A Complete Beginner's Guide", November 2015, https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283/. See also: Q. SHENTU and J. YU, "Research on Anonymization and De-anonymization in the Bitcoin System", October 2015 (electronically available via https://arxiv.org/pdf/1510.07782.pdf).

148 See: http://ethdocs.org/en/latest/introduction/history-of-ethereum.html.

149 See: https://www.ethereum.org.

Ethereum has a capability that goes far beyond that of a pure P2P digital cash equivalent like Bitcoin. In simple terms, it is much like a smartphone operating system on top of which software applications can be built.[150]

Technically speaking, the Ethereum platform itself is not a cryptocurrency. However, like other open, permissioneless blockchains, Ethereum requires a form of on-chain value to incentivise transaction validation within the network (i.e. a form of payment for the network nodes that execute the operations).[151] This is where Ethereum's native cryptocurrency "ether" (ETH) comes into play. Ether does not only allow smart contracts to be built on the Ethereum platform (i.e. it fuels them[152]), but it also functions as a medium of exchange (specifically in the context of ITOs, as many tokens are bought with ether).

Like Bitcoin, Ethereum currently utilises a PoW consensus mechanism, but it is slowly moving towards the adoption of a PoS consensus mechanism[153], better known as the Casper Protocol.[154]

Ethereum's development is promoted and supported by the "Ethereum Foundation"[155], a Swiss non-profit organization, founded by Ethereum's inventors. A large bulk of ether was "pre-mined" (i.e. mined / created before the coin was officially launched to the public[156]) by its inventors and sold in a crowdsale to pay for development costs and fund the Ethereum Foundation.[157]

b. Ethereum runs on an open, permissionless blockchain

Just like Bitcoin, Ethereum is a prominent example of an open, permissionless blockchain. Anyone can join or leave the Ethereum network at will, without having to be pre-approved by any entity.

c. Ether (ETH) is directly convertible into fiat currency

Ether (ETH) can be bought with and converted into fiat currency on various cryptocurrency exchanges (e.g. Coinbase, Kraken, …).

d. Ether (ETH) is a medium of exchange

Like Bitcoin, ether (ETH) is being accepted as a means of payment by a growing number of merchants (e.g. TapJets[158], Overstock[159], …). It is therefore also a medium of exchange.

e. Ether (ETH) is a pseudo-anonymous coin

Just like Bitcoin, ether (ETH) can be categorised as a pseudo-anonymous or pseudonymous coin.[160]

---

150 See: EY, "IFRS – Accounting for crypto-assets", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 4.

151 *Ibid.*

152 *Cf.* G. HILEMAN and M. RAUCHS, "Global Cryptocurrency Benchmarking Study", Cambridge Centre for Alternative Finance, 2017, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, 17.

153 That is, if the nodes in the network reach a consensus regarding this change. If they do not, a hard fork of the Ethereum blockchain could arise. See for more information on this concept further below. See also: https://www.ethereum.org/ether.

154 See for example: A. ROSIC, "What is Ethereum Casper Protocol? Crash Course", November 2017, https://blockgeeks.com/guides/ethereum-casper/.

155 See: https://www.ethereum.org/foundation.

156 See: https://www.investopedia.com/terms/p/premining.asp.

157 See: https://www.ethereum.org/ether.

158 See: https://www.tapjets.com. See also: A. KAPLAN, "Who accepts Ethereum as payment 2018 (List of companies that accept Ethereum)", May 2018, https://smartereum.com/2072/accepts-ethereum-payment-2018-list-companies-accept-ethereum-mon-may-28/.

159 See: P. RIZZO, "Ether, Litecoin and More: Overstock Now Accepts Cryptocurrencies as Payment", August 2017, https://www.coindesk.com/ether-litecoin-overstock-now-accepts-cryptocurrencies-payment/.

3.2.3. Ripple (XRP)

a. What is Ripple?

Ripple is an open-source, P2P decentalized digital payment platform that allows for near-instantaneous transfers of currency regardless of their form (e.g. US Dollar, Yen, Bitcoin, …).[161] It was launched in 2012 by the private company Ripple (Labs), Inc.[162] Ripple (Labs), Inc., responsible for the further development of the Ripple protocol, is the first ever company to have received a "BitLicense" for an institutional use case of digital assets from New York's Department of Financial Services.[163] It is also getting support from a number of big players in the financial services industry, such as Bank of America Merill Lynch, Santander, etc.[164]

Following Ripple's establishment, Ripple's inventors launched the cryptocurrency XRP. XRP was built to become a bridge currency to allow financial institutions to settle cross-border payments a lot faster and cheaper than they can using the global payment networks that are in place today, which can be slow and involve multiple middlemen (i.e. banks).[165] However, in practice, Ripple's payment platform does not need a bridge currency to actually work.[166]

According to Ripple, XRP can handle more than 1,500 transactions per second.[167] While it was initially developed and intended for enterprise use[168], it has meanwhile been adopted by a large number of cryptocurrency users. Ripple (XRP) is not based on a PoW or a PoS mechanism to validate transactions, but it makes use of its own specific consensus protocol.[169]

The total supply of XRP has been fully "pre-mined" (or better: created upon the coin's inception) by its inventors. At present, it is held as follows[170]:

- 8,102,265,714 XRP is held by Ripple (Labs), Inc.;
- 39,189,968,239 XRP has been distributed[171]; and
- 52,700,000,024 XRP has been placed in escrow to create certainty of XRP supply at any given time[172].

---

160 See *inter alia*: C. DANNEN, *Introducing Ethereum and Solidity – Foundations of Cryptocurrency and Blockchain Programming for Beginners*, Apress, 2017, 45; https://ethereumprice.org/what-is-ethereum/; A. MADEIRA, "How to make an anonymous ether transaction using WeiMixer", May 2018, https://www.cryptocompare.com/coins/guides/how-to-make-an-anonymous-ether-transaction/.

161 See: https://ripple.com/xrp/.

162 See: Company Overview of Ripple Labs, Inc., https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=235707311.

163 See: https://ripple.com/insights/ripple-receives-new-yorks-first-bitlicense-institutional-use-case-digital-assets/.

164 See: https://ripple.com/use-cases/banks/.

165 See: M. ORCUTT, "No, Ripple Isn't the Next Bitcoin", January 2018, https://www.technologyreview.com/s/609958/no-ripple-isnt-the-next-bitcoin/.

166 *Ibid.*

167 See: https://ripple.com/xrp/.

168 *Ibid.*

169 See: https://ripple.com/build/xrp-ledger-consensus-process/.

170 See: https://ripple.com/xrp/market-performance/.

171 It is said that Ripple's founders still hold 20 billions XRP. See for example: M. ORCUTT, "No, Ripple Isn't the Next Bitcoin", January 2018, https://www.technologyreview.com/s/609958/no-ripple-isnt-the-next-bitcoin/.

172 It should be noted that the XRP in this escrow account is indirectely owned by Ripple (Labs), Inc. See: https://ripple.com/insights/ripple-escrows-55-billion-xrp-for-supply-predictability/. On its website, Ripple states: "*We use Escrow to establish 55 contracts of 1 billion XRP each that will expire on the first day of every month from months 0 to 54. As each contract expires, the XRP will become available for Ripple's use. You can expect us to continue to use XRP for incentives to market makers who offer tighter spreads for payments and selling XRP to institutional investors. We'll then return whatever is unused at the end of each month to the back of the escrow rotation. For example, if 500M XRP remain unspent at the end of the first month, those 500M XRP will be placed into a new escrow account set to expire in month 55. For comparison, Ripple has sold on average 300M XRP per month for the past 18 months.*"

Unlike Ethereum's inventors, Ripple's inventors did not sell a portion of XRP via a crowdsale upon XRP's creation to fund Ripple (Labs), Inc. The company was privately funded.[173]

At present, it is not fully transparent how XRP (which is mainly held by Ripple (Labs), Inc.) is or will be further distributed in the future.

b. Ripple runs on a public permissioned blockchain

Unlike Bitcoin and Ethereum, Ripple runs on a permissioned blockchain.[174] This is because Ripple (Labs) Inc., the company behind Ripple (XRP), determines who may act as a transaction validator on its network. The blockchain itself is considered public, as it can be accessed and viewed by anyone.

c. Ripple (XRP) is directly convertible into fiat currency

Like Bitcoin, XRP can be directly converted into fiat currency on various crytocurrency exchanges (e.g. Kraken, LiteBit[175], Anycoin Direct, Bitsane[176], …).

d. Ripple (XRP) is a medium of exchange

Ripple (XRP) is being accepted as a means of payment by a growing number of (online) merchants for various goods and services (e.g. e-cigarettes[177], honey[178], coffee[179], …)[180]. There is recentely even buzz and speculation on the internet that Amazon might be looking to adopt Ripple in the near future.[181]

e. Ripple (XRP) is a pseudo-anoymous coin

Like Bitcoin, Ripple (XRP) can be qualified as a pseudo-anonymous coin.[182]

3.2.4. Bitcoin Cash (BCH)

a. What is Bitcoin Cash?

Bitcoin Cash (BCH) is decentralized P2P digital cash.[183] It was created on the 1st of August 2017 and is based on Bitcoin's original SHA-256 PoW algorithm, yet with some changes to its underlying code. Bitcoin Cash is what is known in the crypto-community as a "hard fork" of the Bitcoin blockchain.[184] It is the result of two very different visions on the future of Bitcoin and the Bitcoin blockchain, whereby

---

[173] See for example: E. SPAVEN, "Online payment network Ripple Labs receives $3.5 Million in new funding", September 2014, https://www.coindesk.com/online-payment-network-ripple-labs-receives-3-5m-new-funding/.

[174] See: World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 12. See also: N. Bauerle, "What is the Difference Between Public and Permissioned Blockchains?", 2017, https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains/.

[175] See: https://www.litebit.eu/.

[176] See: https://bitsane.com/exchange/xrp-eur.

[177] See for example: https://vapourdepot.com/.

[178] See for example: http://drapis.com.

[179] See for example: https://www.cryptomercado.com.

[180] See for an overview: https://www.xrpchat.com/topic/5679-ripple-xrp-merchants-directory/.

[181] See: J. P. NJUI, "Amazon Partnership Speculation High For Ripple (XRP) As Markets Go Crazy", May 2018, https://ethereumworldnews.com/amazon-partnership-speculation-high-for-ripple-xrp-as-markets-go-crazy/.

[182] See: T. SAMEEH, "What If Ripple's Transactions Can Be Fully Anonymous?", May 2017, http://www.livebitcoinnews.com/ripples-transactions-can-fully-anonymous/.

[183] See: https://www.bitcoincash.org/en/.

[184] See: World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 19; EY, "IFRS – Accounting for crypto-assets", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 13.

the Bitcoin blockchain diverged into two potential paths forward.[185] In short, some Bitcoin developers wanted to raise the block size limit from 1MB to 8MB[186], to reduce transaction fees and improve confirmation times, whilst others had different plans.[187] Because the community could not reach a consensus, the new cryptocurrency Bitcoin Cash was created.[188]

Like Bitcoin, Bitcoin Cash makes use of the PoW mechanism, which means that it can be mined. What is particular about Bitcoin Cash however, and is a direct result of the hard fork, is that anyone who held Bitcoin at the time Bitcoin Cash was created (*i.e.* 1st of August 2017 – 13:16 UTC) also became owner of the same amount of Bitcoin Cash.[189] Any Bitcoin acquired after that specific time follows the original path and does not include Bitcoin Cash.

b. Bitcoin Cash runs on an open, permissionless blockchain

In principle, a "hard fork" does not change the nature of a coin's blockchain.[190] In other words, Bitcoin Cash also runs on an open permissionless blockchain, just like Bitcoin.

c. Bitcoin Cash is directly convertible into fiat currency

Like Bitcoin, Bitcoin Cash can be easily converted into fiat currency and vice versa through a number of cryptocurrency exchanges (e.g. Coinbase, Kraken, LiteBit, …).

d. Bitcoin Cash is a medium of exchange

Bitcoin Cash can be used to pay for a growing array of goods and services (e.g. jewelry, food, gaming, telecom, …) on a number of online market places and platforms (e.g. OpenBazaar[191], the accept Bitcoin Cash initiative[192]). As a result, Bitcoin Cash can be qualified as a medium of exchange.

e. Bitcoin Cash is a pseudo-anonymous coin

Although Bitcoin Cash is a hard fork of Bitcoin, it does not differ that much from its original form. It is thus also a pseudo-anonymous coin.[193]

3.2.5. Litecoin (LTC)

a. What is Litecoin?

Like Bitcoin, Litecoin (LTC) is an open-source decentralized P2P cryptocurrency.[194] It was launched in October 2011 and is based on what is known as the Scrypt PoW algorithm, which utilises Bitcoin's

---

185 *Ibid*.

186 A larger block size is capable of holding more transactions per block. See: S. BUCHKO, "How Long do Bitcoin Transactions Take?", December 2017, https://coincentral.com/how-long-do-bitcoin-transfers-take/.

187 *Ibid*.

188 It is important to note that Bitcoin's code is open source. It is managed and updated by volunteers who must achieve consensus among nodes for a change to be adopted. If no consensus can be reached the risk of a hard fork exists. See: EY, "IFRS – Accounting for crypto-assets", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 4.

189 *Ibid*. See also: https://support.coinbase.com/customer/portal/articles/2911542.

190 World Bank Group (H. NATARAJAN, S. KRAUSE, and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 19.

191 See: https://www.openbazaar.org.

192 See: https://acceptbitcoin.cash/.

193 See *inter alia*: https://exmo.com/en/news_view?id=1912.

194 See: https://litecoin.com.

original SHA-256 PoW algorithm.[195] Litecoin is often described as the 'silver' to Bitcoin's gold.[196] Apart from the fact that it uses a different algorithm, it is different from Bitcoin in two ways.

Firstly, and this results from the use of the Scrypt PoW algorithm, Litecoin offers a much faster transaction speed than Bitcoin. The time needed to generate a block on the Bitcoin BC is about ten minutes[197], while the average block creation time on the Litecoin blockchain is approximately 2.5 minutes.[198]

Secondly, the total supply limit of Litecoin is with 84 million coins, much higher than the 21 million supply limit of Bitcoin.[199]

b. Litecoin runs on an open, permissionless blockchain

Just like Bitcoin, Litecoin runons on an open, permissionless blockchain. All that is needed to join the network is a download of the open-source software code.

c. Litecoin is directly convertible into fiat currency

Litecoin can be bought with fiat currency on a number of cryptocurrency exchanges (e.g. BTCDirect[200], LiteBit, Coinbase, Anycoin Direct, …) and can, on those exchanges, just as easily be exchanged for fiat currency.

d. Litecoin is a medium of exchange

Litecoin is accepted as a means of payment by a gradually growing number of online merchants.[201] Like Bitcoin, it thus also constitutes a medium of exchange.

e. Litecoin is a pseudo-anonymous coin

Just like Bitcoin, Litecoin is a pseudo-anonymous coin. Everyone can verify the chain of LTC transactions on the basis of the public ledger, which would make it technically possible to identify the coins sender and/or receiver.[202]

f. Litecoin and the case of "Atomic Swaps"

It should be noted that the Litecoin community recently introduced a new technology into the crypto-world that is being referred to as the "atomic swap". Simply put, an atomic swap enables a P2P cross-chain exchange or trade of one cryptocurrency for another cryptocurrency, without the need of

---

195 A. ROSIC,"What is Litecoin? A Basic Beginners Guide", December 2017, https://blockgeeks.com/guides/litecoin/.

196 B. PETERSON, "The founder of litecoin, a cryptocurrency that has gained 650% in 7 months, told us he's worried about all the scams in the nascent market", January 2018, http://www.businessinsider.com/litecoin-founder-charlie-lee-on-bitcoin-and-the-cryptocurrency-bubble-2018-1?international=true&r=US&IR=T; G. HILEMAN and M. RAUCHS, "Global Cryptocurrency Benchmarking Study", Cambridge Centre for Alternative Finance, 2017, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, 17.

197 A transaction generally needs six confirmations or 'blocks' before its processed. As a result, the time needed to confirm a transaction on the Bitcoin blockchain normally averages around one hour. However, due to Bitcoin's rise in popularity, congestions have arisen on the Bitcoin network. In some cases, transaction times have been reported to exceed several hours. See for example: S. BUCHKO, "How Long do Bitcoin Transactions Take?", December 2017, https://coincentral.com/how-long-do-bitcoin-transfers-take/.

198 It has been argued that the enabling of faster transactions might pose a security issue, since less thorough checks of the data are required. See: J. MARTINDALE, "What is Litecoin? Here's everything you need to know", January 2018, https://www.digitaltrends.com/computing/what-is-litecoin/.

199 *Ibid.*

200 See: https://btcdirect.eu/.

201 See for an overview of online merchants that accept payments in Litecoins: https://litecoin.com/services#merchants.

202 *Cf.* F. ETTO, "Know Your Coins: Public vs. Private Cryptocurrencies", September 2017, https://www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588.

a third-party.[203] For example, if Anna has one Bitcoin and she wants 100 Litecoins in return, she would normally have to go through an exchange (*i.e.* a third-party) and pay certain fees to get this trade done. Suppose that Jeff owns 100 Litecoins and he instead wants one Bitcoin, then with an atomic swap Anna and Jeff could simply trade their Coins with one another.[204] Now, in practice an atomic swap is of course not so easy.

First of all, since it is presently still in its infancy, the implementation of the atomic swap technology requires a lot of IT-knowledge. For example, a link has to be made between the two cryptocurrency blockchains, which requires the implementation of an IT-protocol known in the crypto-community as the "Lightning Protocol".[205] In addition, both blockchains have to share the same cryptographic function (for example the SHA-256 function) in order for the atomic swap to be possible.[206] While we are not there yet in terms of user friendly cross-chain trading, the emergence of the atomic swap technology brings forth a whole new set of challenges.

3.2.6. Stellar (XLM)

a. What is Stellar?

Like Ripple, Stellar is an open-source, distributed payments infrastructure. Stellar was created in 2014 by one of Ripple's founding fathers.[207] Its goal is to connect people to low-cost financial services to fight poverty and develop individual potential.[208] Stellar can also be used to build smart contracts.[209] It is not based on a PoW or PoS consensus mechanism, but has its own specific consensus protocol.

Stellar is home to the cryptocurrency Lumen (XLM). In short, Lumens are used to pay for transactions on the Stellar network; they contribute to the ability to move money around the world and to conduct transactions between different currencies quickly and securely.[210]

Stellar's development is supported by the non-profit organization Stellar.org (incorporated in 2014 as a non-stock nonprofit corporation in the U.S. State of Delaware), which contributes to the development of tools and social good initiatives around the Stellar network and financial inclusion.[211] Its employees contribute code to the network, but the network itself is said to be completely independent of the organization.[212]

Similar to Ripple's cryptocurrency XRP, the total supply of Stellar Lumens is "pre-mined". It is held by Stellar.org who has been given the task to distribute Lumens *for free*, in the following manner[213]:

- 50% is to be given away to individuals (via a direct sign-up program);

---

[203] See: R. ROSE O'LEARY, "Atomic Action: Will 2018 Be the Year of the Cross-Blockchain Swap?", January 2018, https://www.coindesk.com/atomic-action-will-2018-year-cross-blockchain-swap/.

[204] A recent test case completed by the inventor of Litecoin, Mr Charlie Lee, shows that atomic swaps between Litecoin and Bitcoin are indeed possible. See: J. BUCK, "First BTC-LTC Lightning Network Swap Completed, Huge Potential", November 2017, https://cointelegraph.com/news/first-btc-ltc-lightning-network-swap-completed-huge-potential.

[205] A. ROSIC, "What is Litecoin? A Basic Beginners Guide", December 2017, https://blockgeeks.com/guides/litecoin/.

[206] See: B. ASOLO, "What are Atomic Swaps?", May 2018, https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/. This means that theoretically, swaps between a number of Cryptocurrencies could be possible.

[207] See *inter alia*: C. ADAMS, "Stellar Lumens Vs Ripple", March 2018, https://www.investinblockchain.com/stellar-lumens-vs-ripple/; S. TOWN, "Introduction to Stellar Lumens (XLM) – The Future of Banking", April 2018, https://cryptoslate.com/stellar-lumens/.

[208] See: https://www.stellar.org/about/. It should be noted that Stellar's primary target audience (i.e. the individual) is thus totally different from Ripple's (i.e. financial institutions).

[209] See: https://www.stellar.org/developers/guides/walkthroughs/stellar-smart-contracts.html.

[210] See: https://www.stellar.org/lumens/.

[211] See: https://www.stellar.org/about/mandate/.

[212] See: https://www.stellar.org/how-it-works/stellar-basics/.

[213] See: https://www.stellar.org/about/mandate/.

- 25% is to be given away to partners (via a specific partnership program);
- 20% is given away to Bitcoin and XRP holders; and
- 5% is reserved for Stellar.org's operational expenses.

The actual distribution is not conducted at once, but over time in a number of rounds.

b. Stellar runs on a permissionless blockchain

Unlike Ripple, Stellar runs on a permissionless blockchain. Anyone can join the network at will and, if certain conditions are met, validate transactions without having to be pre-approved or vetted by any central administrator.[214]

c. Lumens (XLM) are directly convertible into fiat currency

Lumens (XLM) can be directly converted into fiat currency through cryptocurrency exchanges such as LiteBit (up to a maximum amount of EUR 500 (per transaction)) or Kraken.

d. Lumens (XLM) are NOT a true medium of exchange yet

At present, so it seems, Lumens (XLM) can only be used to pay for promotional Stellar stickers[215], breakfast at a local breakfast bar in Arkansas[216] and sprouts[217]. While this proves that they are gradually being accepted as a means of payment, they are not a true medium of exchange yet, at least not if you compare them to the coins discussed above.

e. Lumens (XLM) are pseudo-anonymous coins

All transactions on the Stellar network are public, but they cannot be linked easily to the identities of their users.[218] As a result, Stellar Lumens (XLM) can be qualified as pseudo-anonymous coins.

3.2.7. Cardano (ADA)

a. What is Cardano?

Like Ethereum, Cardano is designed and being further developed as a platform on top of which smart contracts and decentralized applications (so-called "Dapps") can be run.[219] The Cardano project began in 2015[220], and was officially released to the public in September 2017[221]. It is based on what is known as the Ouroboros PoS algorithm.[222]

---

214 See: https://www.stellar.org/how-it-works/stellar-basics/.

215 See: https://stellar.shop/products.

216 See: https://www.preludebreakfast.com.

217 See: https://www.sproutgrowers.world/product/sprout-grower/.

218 See: https://www.stellar.org/how-it-works/stellar-basics/.

219 See: https://www.cardano.org/en/what-is-cardano/.

220 See: https://www.cardano.org/en/philosophy/.

221 E. POSNAK, "On the Origin of Cardano", December 2017, https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c.

222 See: A. KIAYIAS, A. RUSSEL, B. DAVID and R. OLIYNYKOV, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", August 2017, https://iohk.io/research/papers/?__hstc=64163184.47e0ede3cd3368ac41d33e513fea0c1b.1525905532910.1527544936508.1527699072699.9&__hssc=64163184.7.1527699072699&__hsfp=2761973715#9BKRHCSI.

The Cardano platform is home to the open source decentralized cryptocurrency Ada (ADA).[223] Ada can be used to send and receive digital funds. It fuels the Cardano platform, just like the currency "ether" fuels the Ethereum platform.

In short, Cardano aims to improve scalability, security, governance, and interoperability with traditional financial systems and regulations, by learning from and improving on lessons learned in the Bitcoin and Ethereum communities.[224]

What distinguishes Cardano from Ethereum, and from many other cryptocurrencies, is that it is (one of the first) blockchain projects to be developed and designed from a scientific philosophy by a team of leading academics and engineers.[225] Another notable difference is that, at present, the cryptocurrency Ada (ADA) can only be stored in Cardano's own digital wallet Daedalus.[226]

The Cardano project currently has three main contributors that each have separate roles:

- the Cardano foundation, based in Switzerland, which aims to standardise, protect and promote the Cardano technology and eco-system;
- IOHK, a blockchain engineering company responsible for building the Cardano blockchain; and
- Emurgo, an entity responsible for the fostering of commercial applications being built upon the Cardano ecosystem.

Similar to Ethereum (*cf.* ether), a good number of Ada was "pre-mined" (i.e. mined / created before the coin was launched to the public) by its inventors and sold in a crowdsale to pay for development costs.[227]

b. Cardano runs both permissionless and permissioned blockchains

Cardano's Ouroboros PoS algorithm allows the platform to run both permissionless and permissioned blockchains.[228]

c. Ada (ADA) is directly convertible into fiat currency

The currency Ada (ADA) can be directly converted into fiat currency. However, we found that, at present, only one cryptocurrency exchange offers the option to directly convert Ada (ADA) into Euro, being LiteBit and only up to a maximum amount of EUR 500 (per transaction).

Ada can, on the contrary, easily be exchanged for other cryptocurrencies (for example through an exchange such as Bittrex[229] or Binance). These cryptocurrencies can then be converted into fiat currency.

d. Ada (ADA) is NOT a true medium of exchange yet

Our research shows that, at present, Ada can only be used to pay for a very limited number of services (e.g. Hotel Ginebra Barcelona accepts payment in Ada[230]). While this proves that Ada is gradually

---

223 See: https://www.cardano.org/en/what-is-cardano/.

224 E. POSNAK, "On the Origin of Cardano", December 2017, https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c.

225 See: https://www.cardano.org/en/what-is-cardano/.

226 See: https://www.cardano.org/en/the-daedalus-wallet/.

227 See: https://cardanodocs.com/cardano/monetary-policy/.

228 See: https://whycardano.com. See also: A. Ramesh, "Features of various Blockchains: A Comparison", February 2018, https://www.xoken.org/blog/features-of-various-blockchains-a-comparison/.

229 See: https://bittrex.com/home/markets.

230 See: https://www.hotelginebra.com.es/welcome/ada/.

being accepted as a means of payment, it is not a true medium of exchange yet, at least not if you compare it to the coins discussed above. This could however change fairly quickly.[231]

e. Ada (ADA) is a pseudo-anonymous coin

Just like the cryptocurrencies analysed above, Ada can be qualified as a pseudo-anonymous coin.[232] It is interesting to note however – and as far as we could establish, unparalleled – that know your customer (KYC) standards were applied during the initial offering of Ada.[233]

3.2.8. IOTA (MIOTA)

a. What is IOTA?

IOTA, launched in 2016[234], is an open-source eco-system where people and machines can transfer value (i.e. money) and/or data without any transaction fees in a trustless, permissionless, and decentralized environment.[235]

In short, IOTA employs specific technology that is said to be more scalable than the technology behind most other coins, and promises faster transaction speeds.[236] Like the cryptocurrencies analysed above, IOTA is based on distributed ledger technology. However, unlike those other cryptocurrencies, IOTA's distributed ledger does not consist of transactions grouped into (transaction) "blocks" and stored into sequential chains (i.e. it is not a "blockchain"), but of a stream of individual transactions entangled together.[237] IOTA is based on what is known as a directed acyclic graph (DAG).[238] Because transactions are entangled together, this technology is also being referred to as the "Tangle".[239]

Instead of requiring miners to perform computational PoW and validate transaction blocks in exchange for newly "mined" coins, IOTA's network participants create a consensus themselves by validating two previous transactions each time they wish to make a new transaction.[240]

At present, IOTA is still very much in its infancy. This is reflected, *inter alia*, by the fact that in order to fully secure the network all transactions have to be digitally signed by a special network node (i.e. the "Coordinator"[241]). Because this affects the network's true decentralized nature, IOTA's development team is working hard on an update to remove this special node by the end of 2018.[242]

The IOTA eco-system is being further developed, supported, promoted and maintained by the "IOTA Foundation"[243], a German non-profit foundation, founded by IOTA's inventors. The total supply of

---

231 *Cf.* A. ANTONOVICI, "Cardano's Emurgo and SK's Metaps Plus Partner to Accept ADA", May 2018, https://cryptovest.com/news/cardanos-emurgo-and-sks-metaps-plus-partner-to-accept-ada/.

232 See: https://cardanodocs.com/introduction/#cryptocurrency-basics.

233 See: https://www.cardano.org/en/ada-distribution-audit/.

234 X, "An introduction to IOTA", 2017, https://iotasupport.com/whatisiota.shtml.

235 See: https://www.iota.org/get-started/faqs.

236 *Ibid.*

237 *Ibid.*

238 S. LEE, "Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0", January 2018, https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#68781282180b.

239 See: https://www.iota.org/get-started/faqs.

240 See: S. POPOV, "The Tangle", October 2017, http://iotatoken.com/IOTA_Whitepaper.pdf. See also: L. TENNANT, "Improving the Anonymity of the IOTA Cryptocurrency", October 2017, https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20f91e77e54d88b7644658912c7d/Improving_the_Anonymity_of_the_IOTA_Cryptocurrency.pdf, 1.

241 See: https://www.iota.org/get-started/faqs.

242 *Ibid.*

243 See: https://www.ethereum.org/foundation.

IOTA was created and released to a number of so-called "founder addresses".[244] The majority of it was sold by IOTA's inventors in a crowdsale to pay for development costs and fund the IOTA Foundation.[245]

b. IOTA runs on a permissionless distributed ledger

IOTA is not based on blockchain technology, but constitutes a different application of distributed ledger technology. It is – to put it in the words of its developers – envisaged to be(come) the *public* and *permissionless* backbone protocol for the internet of things that enables true interoperability between all devices.[246]

c. IOTA is directly convertible into fiat currency

The cryptocurrency IOTA (MIOTA) can be directly converted into fiat currency (such as Euro). However, our research shows that, at present, only one cryptocurrency exchange offers the option to directly convert IOTA (MIOTA) into Euro, being CoinFalcon[247].

IOTA can, on the contrary, easily be exchanged for other cryptocurrencies (for example through an exchange such as Binance). These cryptocurrencies can then be converted into fiat currency.

d. IOTA is NOT a medium of exchange

It seems that there are currently no (online) merchants that accept IOTA as a means of payment for certain goods or services. IOTA is thus not a medium of exchange. It cannot be ruled out however, that it may become one in the (near) future.[248]

e. IOTA is a pseudo-anonymous coin

Despite IOTA's unique eco-system, like most cryptocurrencies it has a transparent and publicly available ledger, meaning a IOTA user's counterparty see that user's IOTA balance and parts of IOTA's transaction history.[249] Just like Bitcoin, IOTA can thus be qualified as a pseudo-anonymous coin.

3.2.9. NEO (NEO)

a. What is NEO?

Similar to Ethereum and Cardano, NEO is an open-source blockchain platform on top of which smart contracts and decentralized applications (so-called "Dapps") can be run. NEO, sometimes referred to as the "Chinese Ethereum"[250], was originally launched under the name "Antshares" in February 2014.[251] The project was rebranded "NEO" in June 2017.[252]

---

244 See: X, "IOTA Coin Review", January 2018, https://hackernoon.com/iota-coin-review-6a1c73c5cfa3.

245 X, "An introduction to IOTA", 2017, https://iotasupport.com/whatisiota.shtml.

246 See: https://www.iota.org/get-started/faqs.

247 See: https://coinfalcon.com.

248 *Cf.* L. TENNANT, "Improving the Anonymity of the IOTA Cryptocurrency", October 2017, https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20f91e77e54d88b7644658912c7d/Improving_the_Anonymity_of_the_IOTA_Cryptocurrency.pdf, 2.

249 *Ibid.*

250 See for example: J. TUWINER, "Introduction to NEO – An Open Network For Smart Economy", April 2018, https://cryptoslate.com/introduction-to-neo-an-open-network-for-smart-economy/.

251 See: A. MOSKOV, "Cryptocurrency Industry Spotlight: Who is NEO's Da Hongfei?", January 2018, https://coincentral.com/cryptocurrency-industry-spotlight-neos-da-hongfei/.

252 See: N. LEVENSON, "NEO versus Ethereum: Why NEO might be 2018's strongest cryptocurrency", December 2017, https://hackernoon.com/neo-versus-ethereum-why-neo-might-be-2018s-strongest-cryptocurrency-79956138bea3.

In short, the NEO project is aimed at digitising assets and automating the management of digital assets, in order to create a so-called "smart economy" (i.e. an economy where parties can agree on a contract without the need to trust each other).[253]

Just like Ethereum (*cf.* "ether"), NEO itself is technically not a cryptocurrency. NEO's native currency is called "GAS". In simple terms, GAS is a fee to be paid to be allowed to utilise NEO's network. One could in fact say that it "fuels" the platform. What is particular about the NEO platform (and distinguishes it from the Ethereum and Cardano plaforms) is that holding the digital value "NEO" (which could best be described as some sort of hybrid crypto-asset) automatically generates an amount of GAS over time.[254]

NEO is based on a consensus mechanism known in the crypto-community as the delegated Byzantine Fault Tolerance (dBFT) algorithm, which could potentially support 10.000 transactions per second.[255]

The total supply of NEO was "pre-mined"[256]; half of it was sold in a crowdsale and the other half is managed by the NEO Council (i.e. group of the project's founders) to support development and maintenance of the NEO ecosystem.[257]

b. NEO runs on a permissioned blockchain

In order to become a transaction validator (i.e. a node) on the NEO network, a validator candidate has to be (i) selected by NEO's development team and (ii) voted in by the NEO community (i.e. those who hold NEO).[258] These characteristics are typical for a permissioned blockchain.

c. NEO is directly convertible into fiat currency, GAS is not

NEO can be directly converted into fiat currency. However, our research shows that, at present, only one cryptocurrency exchange offers the option to directly convert NEO into Euro, being Anycoin Direct[259].

NEO's native currency GAS can presently not be directly converted into fiat currency.

Both NEO and GAS can, however, easily be exchanged for other cryptocurrencies (for example through an exchange such as Bittrex). These cryptocurrencies can then be converted into fiat currency.

d. NEO's GAS is NOT a medium of exchange

While NEO is working very closely with big tech companies like Microsoft[260], its native currency GAS is not a medium of exchange (nor is NEO itself). Contrary to a number of other coins discussed above,

---

253 See: https://neo.org. See also: M. LERIDER, "What is NEO Smart Economy?", August 2017, https://medium.com/@MalcolmLerider/what-is-neo-smart-economy-381a4c6ee286.

254 GAS itself can also be individually acquired, for example on the Cryptocurrency Exchange Binance (https://www.binance.com/).

255 See: http://docs.neo.org/en-us/index.html.

256 See *inter alia*: S. KHATWANI, "NEO Cryptocurrency: Everything You Need to Know about China Ethereum", December 2017, https://coinsutra.com/neo-cryptocurrency/; X, "What is NEO, and what is GAS?", September 2017, https://hackernoon.com/what-is-neo-and-what-is-gas-5b9828a1aa65.

257 X, "What is NEO, and what is GAS?", September 2017, https://hackernoon.com/what-is-neo-and-what-is-gas-5b9828a1aa65.

258 See *inter alia*: X, "A Definitive Guide To NEO (2nd Edition)", January 2018, http://storeofvalueblog.com/posts/a-definitive-guide-to-neo/; CITY OF ZION, "Coopetition: A New Approach to Decentralization", December 2017, https://medium.com/proof-of-working/decentralization-from-coopetition-b10d7ce3b9d.

259 It should be noted that "on paper" the cryptocurrency exchange Bitfinex (https://www.bitfinex.com) also offers the option to convert NEO into Euro. However, in practise it proves to be very difficult (to impossible) to actually withdraw such funds from the plaform.

260 See for example: H. NASEER, "NEO Launches Dev Competition with $490,000 Prize Pool, Co-organized by Microsoft", November 2017, https://cryptovest.com/news/neo-launches-dev-competition-with-490000-prize-pool-co-organized-by-microsoft/; W. SUBERG, "NEO

our research did not reveal any online merchants willing to accept NEO's coins as a means of payment. Some argue that GAS is in fact not really intended to be a true medium of exchange.[261] However, the same was also said for Ethereum's currency ether (ETH). With that in mind, it cannot be entirely ruled out that GAS (or even NEO itself) may still become a medium of exchange in the future.

e. NEO's GAS is a pseudo-anonymous coin

In essence, NEO's GAS could be qualified as a pseudo-anonymous or pseudonymous coin, just like the coins analysed above. However, NEO's core developers are currently actively working on a concept that would allow coders of smart contracts to tie a so-called "digital identity" to a real world identity.[262] It is not entirely inconceivable – yet at this time still highly unclear – that this technology will also impact GAS's pseudo-anonymous character.[263]

3.2.10. Monero (XMR)

a. What is Monero?

Monero (XMR) is an open-source P2P cryptocurrency *"with a focus on private and censorship-resistant transactions"*.[264] It was launched in April 2014[265] and is based on what is known as the CryptoNote[266] PoW algorithm.

Monero has been specifically developed to allow its users to execute transactions in full anonymity. It is said to be cryptographically private by default.[267] In particular, it uses cryptography to shield both sending and receiving addresses (*i.e.* so-called 'keys'[268]), as well as transacted amounts.

Monero (XMR) is characterized as being fully fungible. This means that two units of XMR can always be mutually substituted and there can be no blacklisting of certain units of XMR by vendors or exchanges due to their association in previous transactions.[269] Non-fungible cryptocurrencies, like Bitcoin and Litecoin, are theoretically susceptible to blacklisting; if they have been used for an illegal purpose in the past, then such history will be contained in the blockchain forever.

Unlike some other Coins, Monero (XMR) has not been pre-mined.

b. Monero runs on a permissionless blockchain

Just like Bitcoin, Monero (XMR) runs on a permissionless blockchain.[270] Anyone can join the network at will, without having to be pre-approved or vetted by any central administrator.

DevCon Sees Microsoft Judge Network's Potential Uses", November 2017, https://cointelegraph.com/news/neo-devcon-sees-microsoft-judge-networks-potential-uses.

261 See: https://www.reddit.com/r/NEO/comments/6su31n/here_are_some_things_you_should_know_if_you_are/; M. LERIDER, "Clarification on NEO, GAS and Consensus Nodes", August 2017, https://medium.com/@MalcolmLerider/clarification-on-neo-gas-and-consensus-nodes-aa94d4f4b09.

262 See: https://neo.org.

263 See for a more elaborate analysis and discussion of this technology: K. SOETEMAN, "Werking dBft via Neo in kaart gebracht", February 2018, https://www.computable.nl/artikel/achtergrond/technologie/6306817/5182002/werking-dbft-via-neo-in-kaart-gebracht.html.

264 See: https://getmonero.org/get-started/what-is-monero/.

265 See: https://getmonero.org/resources/about/. See also: C. BOVAIRD, "What to know before trading Monero", May 2017, https://www.coindesk.com/what-to-know-before-trading-monero/.

266 See: https://cryptonote.org/whitepaper.pdf.

267 A. ZAINUDDIN, "Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies", 2017, https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/.

268 Also see above under 2.1.2. How a blockchain works: the basics.

269 See: https://getmonero.org/resources/moneropedia/fungibility.html.

270 See: https://getmonero.org/resources/moneropedia/cryptocurrency.html.

c. Monero is directly convertible into fiat currency

Monero (XMR) can be directly converted into fiat currency on a number of cryptocurrency exchanges (e.g. LiteBit, Anycoin Direct, Kraken, …).

d. Monero is a medium of exchange

Monero is accepted as a means of payment by a gradually growing number of online merchants.[271] Like Bitcoin, it thus also constitutes a medium of exchange.

e. Monero is an anonymous coin

On a fully transparent blockchain, such as the Bitcoin or Ethereum blockchain, transactions are always openly verifiable and traceable by anyone. In practice – though this will be no easy task – the sending and receiving addresses for such transactions could also be linked to a person's real-life identity.[272] This is where Monero advocates to be different. It positions itself as a secure, private and untraceable cryptocurrency.

This high standard of anonymity is achieved using two different techniques:

- Ring Confidential Transactions ("**RingCT**"); and
- Stealth addresses.

i. Ring Confidential Transactions

Firstly, Monero makes use of so-called Ring Confidential Transactions. RingCT combine the technique of ring signatures and what is referred to in the crypto-community as the confidential transactions concept:

- Ring signatures combine or 'mix' a user's account keys with public keys obtained from Monero's blockchain to create, what could be called a 'ring' of possible signers[273], meaning outside observers cannot link a signature to a specific user.[274] Combined with stealth addresses (see below) they allow to fully obscure the identify of both senders and recipients of XMR;
- Confidential transactions add another layer of privacy to the 'mix' by also concealing the amount of each transaction.[275] Without revealing the actual numbers, they include a cryptographic proof that the sum of the input amounts is the same as the sum of the output amounts.[276]

ii. Stealth Addresses

Secondly, and in addition to RingCT, Monero also makes use of stealth addresses. Stealth addresses are randomly generated, one-time addresses created for each transaction made by the sender on behalf of the recipient. All payments sent to the recipient are routed through these addresses, ensuring there are no links on the blockchain between the sender's and the recipient's address.[277] In

---

271 See for an overview of online merchants that accept payments in Monero: https://getmonero.org/community/merchants/.

272 N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 57. Also see above under 3.2.1. Bitcoin (BTC).

273 See for more information on this concept: https://people.csail.mit.edu/rivest/pubs/RST01.pdf.

274 C. BOVAIRD, "What to know before trading Monero", May 2017, https://www.coindesk.com/what-to-know-before-trading-monero/.

275 See for more information on this concept: https://people.xiph.org/~greg/confidential_values.txt.

276 A. ZAINUDDIN, "Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies", 2017, https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/.

277 *Ibid.*

other words, stealth addresses prevent linkability on the blockchain. However, without the use of RingCT, the original sender of the coins would still be able to trace the coins if they would be moved by the recipient by identifying outputs on the blockchain. RingCT masks these outputs, making the transaction entirely untraceable.[278]

iii. The Kovri-Project

It should be noted that the community of (core) developers and cryptography experts behind Monero is currently working on a project to add yet another layer of privacy to the Monero eco-system by routing and encrypting XMR transactions via I2P Invisible Internet Project nodes.[279] The use of I2P will obfuscate a transactor's IP address and provide further protection against network monitoring.

This project, of which an alpha version is currently in the works, is better known in the crypto-community as the Kovri-project.

[278] See: C. BOVAIRD, "What to know before trading Monero", May 2017, https://www.coindesk.com/what-to-know-before-trading-monero/.

[279] "*I2P is an anonymous overlay network - a network within a network. It is intended to protect communication from dragnet surveillance and monitoring by third parties such as Internet Service Providers*" – see: https://geti2p.net/en/.

Box 1: The Kovri-project

"Kovri uses (...) encryption and (…) routing to create a private, protected overlay-network across the internet. This overlay-network provides users with the ability ***to effectively hide their geographical location and internet IP address****. Essentially, Kovri covers an application's internet traffic to make it anonymous within the network."* (own emphasis added)

Source: https://getkovri.org.

3.2.11. Dash (DASH)

a. What is Dash?

Dash (DASH), formerly known as Darkcoin[280], is an open source P2P privacy-centric cryptocurrency.[281] It was first launched in January 2014 and is based on what is known as the X11 PoW algorithm.[282] What is specific to Dash, and makes it different from most other coins, is that it has a two-tier network. Dash's blockchain is secured via so-called "masternodes" in addition to the PoW done by miners.[283]

In short, a masternode is a server connected to the Dash network which guarantees a certain minimum level of performance and functionality to perform certain tasks related to PrivateSend and InstantSend (Dash's anonymity and instant transaction features).[284]

Transactions with traditional cryptocurrencies can be very time-consuming (i.e. they can take anywhere between a few minutes and more than one hour). This is due to the fact that enough blocks have to pass to ensure that a transaction is irreversible and at the same time not an attempt to double-spend money that has already been spent.[285] Dash tackles this issue utilising its masternode network. Masternodes can be called upon to form voting quorums to check whether or not a submitted transaction is valid and if it is, "*the masternodes 'lock' the inputs for the transaction and broadcast this information to the network, effectively promising that the transaction will be included in subsequently mined blocks and not allowing any other spending of these inputs during the confirmation time period*".[286] As a result Dash is said to be able to compete with nearly instantaneous transaction systems, such as credit cards.[287]

b. Dash runs on an open, permissionless blockchain

Like Monero, Dash runs on a permissionless blockchain.[288] Anyone can join the network at will, without having to be pre-approved or vetted by any central administrator.

c. Dash is directly convertible into fiat currency

Dash (DASH) can be directly converted into fiat currency through various cryptocurrency exchanges (e.g. Anycoin Direct, Kraken, …).

---

280 S. HIGGINS, "How True Anonymity Made Darkcoin King of the Altcoins", May 2014, https://www.coindesk.com/true-anonymity-darkcoin-king-altcoins/.

281 See Dash whitepaper: https://github.com/dashpay/dash/wiki/Whitepaper.

282 See: https://docs.dash.org/en/latest/introduction/features.html.

283 See: https://docs.dash.org/en/latest/masternodes/understanding.html.

284 *Ibid.*

285 See: https://docs.dash.org/en/latest/introduction/features.html#instantsend.

286 *Ibid.*

287 *Ibid.*

288 See: S. GOLDBERG, "Mythbusting: Blockchain and Cryptocurrencies Edition", May 2018, http://paymentsjournal.com/mythbusting-blockchain-and-cryptocurrencies-edition/.

d. Dash is a medium of exchange

Just like Monero, Dash is being accepted as a means of payment by a steadily growing number of online merchants.[289] As a result Dash also constitutes a medium of exchange.

e. Dash is an (optional) anonymous coin

Like Bitcoin's blockchain, Dash's blockchain is transparent by default, which means that generally speaking transactions are always openly verifiable and traceable on the blockchain. To give its users true financial privacy, Dash offers the option to use a feature called PrivateSend. PrivateSend obscures the origins of a user's funds through a process known as "mixing".[290]

Box 2: The PrivateSend mixing-process explained

"1. PrivateSend begins by breaking your transaction inputs down into standard denominations. These denominations are 0.01 Dash, 0.1 DASH, 1 DASH and 10 DASH – much like the paper money you use every day.

2. Your wallet then sends requests to specially configured software nodes on the network, called 'masternodes'. These masternodes are informed then that you are interested in mixing a certain denomination. No identifiable information is sent to the masternodes, so they never know 'who' you are.

3. When two other people send similar messages, indicating that they wish to mix the same denomination, a mixing session begins. The masternode mixes up the inputs and instructs all three users' wallets to pay the now-transformed input back to themselves. Your wallet pays that denomination directly to itself, but in a different address (called a change address).

4. In order to fully obscure your funds, your wallet must repeat this process a number of times with each denomination. Each time the process is completed, it's called a 'round'. Each round of PrivateSend makes it exponentially more difficult to determine where your funds originated. The user may choose between 2-8 rounds of mixing.

5. This mixing process happens in the background without any intervention on your part. When you wish to make a transaction, your funds will already be anonymized. No additional waiting is required."

Source: https://docs.dash.org/en/latest/introduction/features.html#privatesend.

3.3. Conclusion: a taxonomy and timeline of cryptocurrencies

On the basis of the above overview and the above analysis we come to a taxonomy and timeline of cryptocurrencies, allowing to more precisely conduct the regulatory analysis and to signal the flaws of the regulatory framework hereinafter.

We start with the taxonomy.

What is clear from the overview is that THE cryptocurrency is non existing. Although some are similar to each other, there is a lot of variation as to how they are structured, on which technology they run, the anonymity involved, etc.

The below table intends to illustrate this diversity. The selected cryptocurrencies are compared on the basis of various parameters: whether they run on permissioned or permissionless technology, their decentralized nature, whether they were initially offered by an identifiable person or entity, if they are electronically traded, directly convertible into fiat currency, are a medium of exchange and are pseudo-anonymous or fully anonymous. These parameters are not chosen randomly, but help to

[289] See for an overview of online merchants that accept payments in Dash: https://www.dash.org/merchants/.

[290] See: https://docs.dash.org/en/latest/introduction/features.html#privatesend.

assess hereinafter to what extent the cryptocurrencies are caught by AMLD5, which crypto players are included in the scope of AMLD5, whether regulation can be attached to relevant players that are not (yet) in scope, etc.

The table reflects our understanding of the selected cryptocurrencies. It should be read mindful of the fact that making clear-cut distinctions between cryptocurrencies is not easy.[291] Complicating factors are *inter alia* the scarcity of the information available and the often highly technical nature thereof. Moreover, cryptocurrencies are a moving target. E.g. a cryptocurrency that is not a medium of exchange now, can be one tomorrow. Therefore, the overview does not pretend to be the only way of portraying or classifying the selected cryptocurrencies.

Arguably, to get an absolutely clear picture of cryptocurrencies and all their different features in view of giving the best possible policy advice, more work needs to be done and further research is required. Nevertheless, for the purposes of this study, we are of the opinion that below table is a workable instrument, allowing to draw some conclusions throughout the regulatory analysis.

[291] Sometimes it is even not easy to make a clear-cut distinction between the technology a coin runs on and the coin itself.

Table 2: Coin taxonomy

Name	Permissionless / Permissioned	Decentralized	Initial offering by an identifiable person or entity?	Electronically traded	Directly convertible into fiat currency	Medium of exchange	Pseudo-anonymous / Anonymous
Bitcoin	Permissionless	✓	✗	✓	✓	✓	Pseudo-anonymous
Ethereum	Permissionless	✓	✓	✓	✓	✓	Pseudo-anonymous
Ripple	Permissioned	✓	✓	✓	✓	✓	Pseudo-anonymous
Bitcoin Cash	Permissionless	✓	✗	✓	✓	✓	Pseudo-anonymous
Litecoin	Permissionless	✓	✗	✓	✓	✓	Pseudo-anonymous
Stellar	Permissionless	✓	✓	✓	✓	✓	Pseudo-anonymous
Cardano	Permissioned / Permissionless	✓	✓	✓	✓	✓	Pseudo-anonymous
IOTA	Permissionless	✓	✓	✓	✓	✗	Pseudo-anonymous
NEO	Permissioned	✓	✓	✓	✓	✗	Pseudo-anonymous
Monero	Permissionless	✓	✗	✓	✓	✓	Anonymous
Dash	Permissionless	✓	✗	✓	✓	✓	Anonymous

Legend:

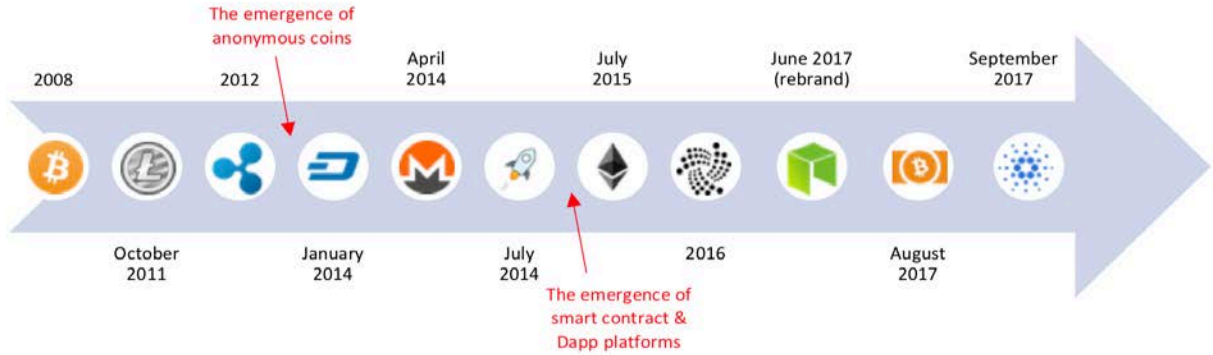
✓ = Yes

✓ = To a limited extent

✗ = No

Moving on to a timeline of cryptocurrencies, further contributing to a better understanding of these coins for regulatory purposes. We observed the following. Where the first cryptocurrencies were developed as pure P2P digital cash equivalents, the analysis above shows that novel forms of cryptocurrencies have meanwhile been created to serve different and /or additional purposes. In 2014 we saw the emergence of cryptocurrencies advocated to be fully anonymous. In 2015 a crucial tipping point appears to have been the creation of the Ethereum platform, which initiated the development of completely new ecosystems or platforms on top of which so-called smart contracts and/or decentralized applications ("Dapps") can be run, fueled by a new generation of cryptocurrencies. This ever-growing technological complexity and evolving nature of cryptocurrencies[292], as illustrated in the timeline included as Figure 2 below, should be taken heed of when further regulating cryptocurrencies in the future.[293]

Figure 2: Coin timeline



[292] See on this evolution also very comprehensive: U. SAIDOV, "Cryptocurrencies: The Rise of Decentralized Money", April 2018, https://blogs.cfainstitute.org/investor/2018/04/03/cryptocurrencies-the-rise-of-decentralized-money/.

[293] It should also be noted that even coins that where originally conceived as pure P2P digital cash equivalents are being further developed by their respective communities and may hold additional features in the future.

4. EU REGULATORY FRAMEWORK

4.1. Setting the scene: similar regulatory challenges in the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies

4.1.1. Anonymity

The key issue that needs to be addressed in order to adequately capture cryptocurrencies and cryptocurrency players, particularly users, in legislation is to unveil the anonymity, varying from complete anonymity to pseudo-anonymity, that surrounds them.[294] This is the biggest problem for combating money laundering and countering terrorist financing: the anonymity prevents cryptocurrency transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter, allowing criminal organisations to use cryptocurrencies to obtain easy access to "clean cash" (both cash in/out). Relating to terrorist financing, the story of Ali Shukri Amin who provided instructions over Twitter on how to use Bitcoin to mask the provision of funds to Daesh is a striking example of the risks brought by the anonymity surrounding cryptocurrencies.[295]

Anonymity is also the major issue when it comes to tax evasion. Entering into taxable cryptocurrency transactions without paying taxes is tax evasion. But, when a tax authority does not know who enters into the taxable transaction, because of the anonymity involved, it cannot detect nor sanction this tax evasion. This makes cryptocurrencies a very attractive means for tax evaders.[296] By some commentators instruments such as Bitcoin were even described as "tomorrow's tax havens".[297]

This being said, and as apparent from our overview of cryptocurrencies above, it should be noted that some cryptocurrencies are pseudo-anonymous, which basically means that if great effort is made[298] and complex techniques are deployed, it is possible for authorities to find out users' identities. Although this can already be a help in the fight against money laundering, terrorist financing and tax evasion in some cases, it does not allow a standardized approach to tackle money laundering, terrorist financing and tax evasion more widely: discovering identities in this way is too complex and costly to become the general answer to tackling this issue - and moreover, it will not certainly lead to any result. New initiatives like the Investigation of Transactions in Underground Markets ("***TITANIUM***") project[299], may change this at some point, but it is still to early to tell to what extent. In any event, a more structural regulatory approach is desirable.

---

[294] IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 27.

[295] FATF, "Report on emerging terrorist financing risks", October 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf, 36.

[296] IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 27; OECD, "Tax Challenges Arising from Digitalisation – Interim Report", 2018, 206, No. 501; R.M. BRATSPIES, "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 43 (electronically available via https://ssrn.com/abstract=3141605).

[297] T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, https://digitalcommons.law.msu.edu/jbsl/vol15/iss2/, 188 and the references there.

[298] The emergence of quantum computing, which uses the laws of quantum mechanics to process large volumes of information much more efficiently than traditional computing, may be able to change this. However, this is not something investigators will be able to apply tomorrow. At present, quantum computing still remains at an embryonic stage of theoretical development. See for an introduction to this technology: B. DUPONT, "The cyber security environment to 2022 Trends, drivers and implications", a study prepared for The National Cyber Security Directorate, Public Safety Canada, 2012, 44p. (electronically available via http://ssrn.com/abstract=2208548).

[299] See: https://www.titanium-project.eu. See also T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens'

Box 3: Some thoughts on the TITANIUM project

The TITANIUM project will research, develop, and validate novel data-driven techniques and solutions designed to support law enforcement agencies charged with investigating criminal or terrorist activities involving virtual currencies and/or underground markets in the darknet. The expected result of the project is a set of services and forensic tools, which operate within a privacy and data protection environment that is configurable to local legal requirements, and can be used by investigators for *inter alia* analyzing transactions across different virtual currency ledgers.

It is clear that the TITANIUM project is directly relevant for the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies. If successful, it will add to the toolbox of law enforcement agencies tracking down money laundering, terrorist financing and tax evasion via cryptocurrencies. Interesting will be to see whether the new techniques developed are less complex and costly than the once already available to trace criminals using pseudo-anonymous cryptocurrencies. Probably we can only speak of significant progress if the outcome would be that law enforcement agencies would have at their disposal an easy to use and relatively cheap method to trace criminals using cryptocurrencies. It will also be interesting to find out whether the new techniques can be deployed both to pseudo anonymous and fully anonymous coins.

In any event, and without prejudice to the TITANIUM project being extremely relevant and valuable, it is not something we can suffice with. As we will evidence throughout this research, there is also a need for a more structural, regulatory approach. It goes without saying that such approach and enhancing the toolbox of law enforcement agencies on the basis of the TITANIUM project go hand in hand: to ensure compliance with the regulatory framework, law enforcement agencies must be able to adequately detect infractions (via the newly developed techniques) and subsequently sanction them.

4.1.2. Cross-border nature

In addition to anonymity, the intrinsically cross-border nature of cryptocurrencies, crypto markets and crypto players is a major challenge for regulators.[300] One of the issues is e.g. that crypto markets and crypto players can be located in jurisdictions that do not have effective money laundering and terrorist financing controls in place.[301] The cross-border nature of cryptocurrencies, crypto markets and crypto players probably means that rules will only be adequate when they are taken at a sufficiently international level.

4.1.3. Often no central intermediary

Another factor of importance challenging the fight against money laundering, terrorist financing and tax evasion is that there is often no central intermediary, such as an issuer, that would normally be the focal point of regulation.[302] Therefore, an important question is to which players in the crypto market should regulation be attached, absent a central intermediary.

4.1.4. Cryptocurrencies are falling between the cracks

The existing European legal framework is failing to deal with the aforementioned issues. There are simply no rules unveiling the anonymity associated with crypto-currencies, making the question whether they are taken at the right level or to whom they apply a superfluous one.

Because of the absence of rules unveiling anonymity, more substantive rules that currently could already have cryptocurrencies in scope completely miss effect. This is particularly true for the legal

Rights and Constitutional Affairs, May 2018, 59 (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

300 IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 25 and 27.

301 ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 28.

302 IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 25.

framework on exchange of information in the field of taxation.[303] The framework simply cannot be activated: to exchange information, authorities must have it in the first place. For the same reasons, the current EU framework on tax avoidance[304], relating *inter alia* to exit taxes in the context of assets transfers by corporates, miss effect when it comes to cryptocurrencies, because of their anonymous and easy-to-hide nature. To be able to tax, the tax administration should know of the taxable basis and when it comes to cryptocurrencies this is just extremely difficult.

Another example relates to the freezing and confiscation of property. Substantively, it is arguable that cryptocurrencies are already in scope of the relevant European rules.[305] Property within these rules refers to property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title or interest in such property. Well, it is acceptable that cryptocurrencies are within the remit of this definition: they could be seen as incorporeal moveable property. Yet, leaving a few examples of success stories aside, the rules largely miss effect. The reason, again, is the same: to be able to freeze and confiscate cryptocurrencies it is necessary to know that a criminal has them, and this is what the anonymity surrounding cryptocurrencies prevents.

So, the crux of the matter is how we can unveil the anonymity related to cryptocurrency transactions so as to be able to track the illegal transactions.

4.1.5. A difficult dividing line with cybersecurity, data protection and privacy

It is accepted that encryption, which is basically what happens in the context of cryptocurrencies, is an effective way for citizens and businesses to defend themselves against the abuse of IT technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information. However, encryption can also be used by criminals, e.g. the use of cryptocurrencies for money laundering or terrorist financing, complicating law enforcement authorities' criminal investigations. Therefore, it is a thin line between preserving strong encryption for the protection of cybersecurity, data protection and privacy on the one hand, while offering opportunities for legitimate law enforcement access to information for the purpose of criminal investigations with appropriate safeguards on the other hand, as was recognized by the European Commission.[306] We raise this issue, but will not elaborate on cybersecurity, data protection and privacy aspects in this research. That would exceed the scope.[307]

---

[303] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, as amended from to time, as regards mandatory automatic exchange of information in the field of taxation; this Directive was very recently, on 25 May 2018, amended again with rules relating to the mandatory automatic exchange of information in the field of taxation for reportable cross-border arrangements and reporting duties of intermediaries (see a first analysis: https://www.tiberghien.com/en/1282/new-reporting-obligation-for-cross-border-arrangements-council-directive-approved-25-may-2018).

[304] Council Directive (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market, *OJ L* 193, 19 July 2016 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1164&from=EN).

[305] The current EU legal framework on the freezing and confiscation of proceeds of crime consists of four Council Framework Decisions (FD) and one Council Decision: Framework Decision 2001/500/JHA13, Framework Decision 2005/212/JHA15, Framework Decision 2003/577/JHA17, Framework Decision 2006/783/JHA18 and Council Decision 2007/845/JHA19. Also see the proposal for a directive on the freezing and confiscation of proceeds of crime in the European Union of 12 March 2012, COM(2012) 85 final and the proposal for a regulation on the mutual recognition of freezing and confiscation orders, COM/2016/0819 final.

Besides, without going into detail on the scope of the whole European substantial framework relating to financial crimes, generally speaking that framework has a broad reach. Therefore, the conclusion we made for freezing and confiscation of property (its scope being large enough already to capture cryptocurrencies), could very well also apply to the larger framework.

[306] See: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en.

[307] On the interaction between blockchain and the GDPR, see *inter alia* M. FINCK, "Blockchains and Data Protection in the European Union", Max Planck Institute for Innovation & Competition Research Paper No. 18-01, 30 November 2017, 32p. (electronically available via https://ssrn.com/abstract=3080322); W. MAXWELL and J. SALMON, "A guide to blockchain and data protection", Hogan Lovells, September 2017, 22p., https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf?_sm_au_=iVV6bs5Z45DMRVfr; A. VAN HUMBEECK, "The Blockchain-GDPR Paradox", November 2017, https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-

4.1.6. Don't throw the baby out with the bathwater: the technology

Cryptocurrencies run on ingenuous technology. From a law enforcement perspective, introducing mechanisms of accountability of crypto players should prevent this technology from being used largely for nefarious purposes, but at the same time not prevent technological innovation from happening[308]. Therefore, legislative action should always be proportionate so that it addresses the illicit behaviour while at the same time not strangling technological innovation at birth. This is an aspect of particular relevance for this research. Cryptocurrencies run on blockchain or other technology. This technology is perfectly legitimate and offers many advantages for innovation in multiple legitimate sectors, including the business and public sector. It has for instance been suggested that blockchain technology could be an adequate defense mechanism against digital ransomware[309]. The idea is that through blockchain technology sensitive information can be kept in a decentralized manner instead of centralized (as it is now). Keeping information in a decentralized manner makes it harder to link the information to the person it relates to. It is then also harder to know who to address for the ransom. Moreover, there would be numerous copies of the info, making it extremely difficult for criminals to hold them all to ransom. Another deterring factor could be that attacking a decentralized system of information would be easily visible to its participants.[310] Another example of a legitimate use case of blockchain technology for the greater good can be found in China[311], where blockchain is being used to combat tax fraud in the context of a partnership between Tencent and the Shenzhen national taxation bureau.[312]

If cryptocurrencies are used for criminal purposes, it is therefore not the technology that needs to be addressed. On the contrary, it is the illicit use that should be targeted. Exceptionally, however, an exception can be made in well-defined cases, such as the mixing technique used in the context of Dash and Monero's RingCT[313], stealth addresses and Kovri-project.[314]

---

fc51e663d047; X, "Blockchain en GDPR: een moeilijk huwelijk", May 2018, https://www.techzine.nl/blogs/404986/blockchain-en-gdpr-een-moeilijk-huwelijk.html?redirect=1; S. MARTINET, "GDPR and Blockchain: Is the New EU Data Protection Regulation a Threat or an Incentive?", May 2018, https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive.

308 U.W., CHOHAN, "International Law Enforcement Responses to Cryptocurrency Accountability: Interpol Working Group", Discussion Paper, 3 April 2018, 3.

309 Ransomware is the illegal act of restricting access to computer files until a ransom is paid. See: X, "True scale of Bitcoin ransomware extortion revealed", MIT Technology Review, April 2018, https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/. See also more elaborate: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 17 *et seq.* (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

310 See e.g. T. SERRES, "2017's Ransomware Attacks: Could Blockchain Technology Have Prevented Them?", May 2017, https://medium.com/animal-media/2017s-ransomware-attacks-could-blockchain-technology-have-prevented-them-ed9ca6bf348b.

311 It should be noted that China's approach towards blockchain technology stands in contrast with its strict approach towards cryptocurrency exchanges. China recently introduced a ban on cryptocurrency exchanges to stop all (domestic) cryptocurrency trading. See: S. SETH, "Is Bitcoin Banned in China?", February 2018, https://www.investopedia.com/news/bitcoin-banned-china/; R. PERPER, "China is moving to eliminate all cryptocurrency trading with a ban on foreign exchanges", February 2018, https://www.businessinsider.nl/china-eliminates-all-cryptocurrency-trading-2018-2/?international=true&r=US&_sm_au_=iVV6bs5Z45DMRVfr; W. SUBERG, "Ban Complete: China Blocks Foreign Crypto Exchanges To Counter 'Financial Risks'", February 2018, https://cointelegraph.com/news/ban-complete-china-blocks-foreign-crypto-exchanges-to-counter-financial-risks; S. LENG, "Beijing bans bitcoin, but when did it all go wrong for cryptocurrencies in China?", February 2018, http://www.scmp.com/news/china/economy/article/2132119/beijing-bans-bitcoin-when-did-it-all-go-wrong-cryptocurrencies.

312 See e.g. S. SUNDARARAJAN, "Chinese City to Use Blockchain In Fight Against Tax Evasion", May 2018, https://www.coindesk.com/tencent-partners-with-city-authority-to-combat-tax-evasion-with-blockchain/; J. SHAWDAGOR, "Blockchain Against Tax Fraud As Tencent Partners Up With Shenzhen National Taxation Bureau", May 2018, https://bitrazzi.com/blockchain-against-tax-fraud-as-tencent-partners-up-with-shenzhen-national-taxation-bureau/.

313 This technique is also being applied to other coins. See: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 32 (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

314 See above and below.

This approach is recognized by the European Commission in the build-up to its proposal to amend AMLD4[315], as will be discussed hereinafter. In that context, the Commission stressed that the proposed measures have no negative effects on the benefits and technological advances presented by the distributed ledger technology underlying virtual currencies, including innovative ways for governments to reduce fraud, corruption, error and the cost of paper-intensive processes, set in place new, modern ways in which governments and citizens interact, in terms of data sharing, transparency and trust, and provide novel insights into establishing ownership and provenance for goods and intellectual property.

4.1.7. The tide is changing: AMLD5

As we will analyse further in this research, the European tide is changing. At the time of writing of this research new European rules on money laundering and terrorist financing are in the final phase of being adopted. These rules include measures to pull cryptocurrencies and (some) crypto players out of the regulatory dark. Hence, the regulatory approach taken by the EU is to address cryptocurrencies and crypto players via the rules on money laundering and terrorist financing.

As a final introductory side note, from a conceptual perspective, the EU could have also done this via other types of legislation, such as financial services legislation. That would have also pulled cryptocurrencies and crypto players out of the dark and into the light, and even more, e.g. relevant crypto players would have needed a license.[316] As we will see further on, this option, from a policy perspective, was not preferred at this stage.

Hereinafter we will elaborate on the new European framework on cryptocurrencies and crypto players in the context of combating money laundering and terrorist financing. We will start the analysis by highlighting the background of the legislative framework. After that, we will briefly discuss the current framework. Subsequently, the legislative road to the upcoming framework and the upcoming framework itself will be scrutinized. Lastly, two add-ons to the framework of combating money laundering and terrorist financing will be briefly touched upon, the Funds Transfer Regulation and the Cash Control Regulation, to verify whether cryptocurrencies are in scope of these regulations.

---

[315] COM/2016/0450, "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", 6 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&qid=1523358551244&from=EN.

[316] At present it is generally speaking very difficult, if not impossible, to include cryptocurrencies and players within the existing scope of financial services legislation. A numbers of examples to illustrate this can be given. First, the scope of various rules is connected to the concept financial instruments, such as market abuse rules or MiFID rules. When we look at the definition of "financial instruments", it is very difficult to include cryptocurrencies within that definition. Therefore, cryptocurrencies will probably not be financial instruments. This means that MiFID licensing rules and behavioural rules for that reason alone cannot be attached to cryptocurrency players, such as cryptocurrency exchange platforms or wallet providers. A second example is that of the prospectus regulation. This uses as connecting factor "securities". Taking a close look at the definition of "securities", it seems that cryptocurrencies do not fit easily within this definition. But more importantly, prospectus requirements are connected to an issuer. In the context of cryptocurrencies, there will not be an issuer (yet, sometimes, there is an offeror, to which theoretically rules could be attached; see infra). A third example is that of payment services. In view of the various components of the definition of payment services it seems difficult to include service providers in relation to cryptocurrencies within that definition. Moreover, it can be expected that the provision of services related to payments by a service provider in the framework of cryptocurrency transactions will not constitute his ordinary profession or business, exempting him anyway from the scope of PSD2. Dependent on the circumstances, also the limited network exception could serve as a safe harbour for the offered services. A last example is that of the e-money rules. It is very clear that cryptocurrencies do not fit within the definition of e-money, exempting them from the scope of these rules. See for a regulatory analysis e.g. R. HOUBEN, "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 193-208; P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 77p.; N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 165 *et seq*.

4.2. Money laundering and terrorist financing

4.2.1. Background

The fight against money laundering and terrorism financing is a key priority of the international community, including the EU. It has long been established that money laundering activities are usually carried out in an international context and therefore national measures are not sufficient. The Recommendations of the Financial Action Task Force ("***FATF***") – drawn up in 1990 and revised from time to time – are the cornerstone of the international framework for combating money laundering and terrorist financing. They have been endorsed by over 180 countries, and are universally recognised as setting out the international standards.[317]

The European Union adopted its first Anti-Money Laundering Directive on 10 June 1991 ("***AMLD1***").[318] An anti-money laundering framework at the level of the European Union was needed to coordinate measures across the different Member States and safeguard the stability of the financial system as a whole. This first Anti-Money Laundering Directive was later amended by the second Anti-Money Laundering Directive ("***AMLD2***")[319], before being repealed and replaced by the third Anti-money Laundering Directive ("***AMLD3***").[320] The latter introduced the fight against terrorist financing and included the revised 2003 FATF Recommendations.[321] In February 2012, the FATF published a revised set of its Recommendations.[322] In parallel, the Commission undertook a review of the third Anti-Money Laundering Directive, which needed to be updated and aligned with the 2012 FATF Recommendations. On 20 May 2015 a revised anti-money laundering and counter-terrorism financing framework was adopted which substantially changed the EU's existing legal framework designed to protect the financial system against money laundering and terrorist financing. The revised rules consist of the fourth Anti-Money Laundering Directive ("***AMLD4***")[323] and the EU Funds Transfer Regulation ("***FTR***")[324] and provide for a more targeted and focused risk-based approach.[325] AMLD4 intends to strengthen the existing rules and to make the fight against money laundering and

---

317 FATF, "International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations", February 2012, 7 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

318 Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, *OJ L* 166, 28 June 1991, 77 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31991L0308&from=EN).

319 Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, *OJ L* 344, 28 December 2001, 76, (electronically available via https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF).

320 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *OJ L* 309, 25 November 2005, 15 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN).

321 FATF, "The Forty Recommendations", 20 June 2003, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf.

322 FATF, "International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations", February 2012, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

323 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *OJ L* 141, 5 juni 2015, 73 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=En).

324 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, *OJ L* 141, 5 juni 2015, 1 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847).

325 On this approach, see e.g. E. HERLIN-KARNELL and N. RYDER, "The robustness of EU Financial Crimes Legislation: A Critical review of the EU and UK Anti-Fraud and Money Laundering Scheme", 2017, European Business Law Review, 1-39.

terrorism financing more effective. AMLD4 should have been transposed by Member States on 26 June 2017 at the latest. As of the same date, also the FTR became applicable.

4.2.2. AMLD4

The core principle of AMLD4 is the prohibition of money laundering and terrorist financing.[326]

What is money laundering? Technically, the following conduct is money laundering, when committed intentionally:

a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points a, b and c[327].

In more simple terms money laundering can be explained as the process by which proceeds of criminal activity are "cleaned" and brought into the lawful economy so that their illegal origins are concealed or disguised.[328]

In the application of the definition of money laundering, "*property*" means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets.[329]

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of a third country.[330]

What is terrorist financing? This is defined as the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA on combating terrorism.[331] The offenses referred to are intentional acts which given their nature or context, may seriously damage a country or an international organisation where committed with the aim of seriously intimidating a population, or unduly compelling a government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional,

---

326 Article 1, 1 and 2 AMLD4.

327 Article 1, 3 AMLD4.

328 E.g. I. BANTEKAS and S. NASH, *International Criminal Law*, Routledge-Cavendish, 2007, 247; S. ROYER, "Bitcoins in het Belgische strafrecht en strafprocesrecht", *RW* 2016-17, No. 13, 491. Generally, there are three steps: the placement phase where the profits generated by the criminal activity must be separated from the criminal activity itself (e.g. dirty money is placed with other legitimate money in the system), the layering phase during which steps are taken to disguise the route which the money takes during the laundering process and the integration phase where the money must become available for use by the criminal organisation.

329 Article 3, (3) AMLD4.

330 Article 1, 4 AMLD4.

331 Article 1, 5 AMLD4.

economic or social structures of a country or an international organisation. Are deemed to be terrorist offences: attacks upon a person's life which may cause death, attacks upon the physical integrity of a person, kidnapping or hostage taking, causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss, etc.

A difference between terrorist financing and money laundering is that in the event of terrorist financing, the origin of the funds can be legitimate. It is the destination of the funds, i.e. financing terrorists, that makes the whole deal illegitimate.[332] Money laundering on the contrary is by definition based on another crime which gives rise to the laundering in question.[333]

There is no definition of "*funds*" included in AMLD4. Legal doctrine opines that it should have the same meaning as "*property*" under AMLD4, especially given that such approach would be consistent with the FATF recommendations.[334]

Ratione personae AMLD4 applies to so-called obliged entities. Because these obliged entities are the entry-point for money laundering and terrorist financing requirements, they are sometimes also referred to as the "gatekeepers".[335]

The obliged entities include: credit institutions, financial institutions, a well defined list of natural or legal persons acting in the exercise of their professional activities (under which auditors, external accountants, tax advisors, notaries and other independent legal professionals), trust or company service providers, estate agents, other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10.000 or more and providers of gambling services.[336]

In addition, Member States are required to extend the scope of AMLD4 in whole or in part to professions and categories of undertakings, other than the obliged entities referred to above, which engage in activities which are particularly likely to be used for the purposes of money laundering or terrorist financing.[337] This implies a continuous monitoring by Member States of money laundering and terrorist financing risks within their territory and taking action when they discover vulnerabilities.

When an entity is an obliged entity and thus falls within the remit of AMLD4, it is subject to various requirements, which ultimately aim at tracing financial information and having a deterrent effect on money laundering and terrorist financing.[338]

An important requirement is that obliged entities have to perform customer due diligence when establishing a business relationship, when carrying out an occasional transaction that amounts to EUR 15.000 or more, when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold, when there are doubts about the veracity or adequacy of previously obtained customer identification data, etc.[339] Customer due diligence measures comprise among others identifying the customer and verifying his/her identity, identifying beneficial owners

---

[332] E.g. N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 278.

[333] E. HERLIN-KARNELL and N. RYDER, "The robustness of EU Financial Crimes Legislation: A Critical review of the EU and UK Anti-Fraud and Money Laundering Scheme", European Business Law Review, 2017, No. 4, 1-39.

[334] N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 295.

[335] See: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en.

[336] Article 2, 1 AMLD4.

[337] Article 4 AMLD4.

[338] See: https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/criminal-justice/financial-crime_en.

[339] Article 11 AMLD4.

and taking reasonable measures to verify these persons' identities, conducting ongoing monitoring of the business relationship, the business and risk profile.[340]

Another important requirement is that when obliged entities know, suspect or have reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, they have to inform the competent financial intelligence unit ("***FIU***"), which every Member State must establish in order to prevent, detect and effectively combat money laundering and terrorist financing, and provide it with all necessary information. All suspicious transactions, including attempted transactions, must be reported.[341] The FIU in turn analyses the suspicious transactions. It disseminates the results of its analyses to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing.[342] Because money-laundering and terrorist financing is not bound by borders, it is evident that FIUs have to cooperate and exchange information with each other to the greatest extent possible, regardless of their organisational status.[343]

When obliged entities fail their duties under AMLD4, they can be sanctioned. AMLD4 demands that any such sanction must be effective, proportionate and dissuasive. Furthermore, and more in general, competent authorities should have at their disposal an adequate sanctioning toolbox, as further detailed under AMLD4, enabling them to adequately sanction breaches of the national provisions transposing AMLD4.[344]

An important innovation of AMLD4 is the so-called beneficial ownership register. This relates to the mandatory set-up of a central register[345] comprising info on the beneficial ownership of corporate and other legal entities. When obliged entities are taking customer due diligence measures, the information on beneficial ownership must be provided to them. Also should the information be accesible by competent authorities and FIUs. Other persons than competent authorities and FIUs who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as corruption, tax crimes and fraud, will also be granted access to beneficial ownership information, in accordance with data protection rules.[346]

AMLD4 contains various provisions relating to the relation with high-risk third countries. Firstly, obliged entities must apply an enhanced level of customer due diligence when dealing with natural persons or legal entities established in high-risk third countries identified by the Commission.[347] Furthermore, reliance on third parties established in high-risk third countries is prohibited.[348] AMLD4 is also conscious of the fact that money laundering and terrorist financing are international problems and the effort to combat them should be global. One of the illustrations is that Member States should ensure that their FIUs exchange information freely, spontaneously or upon request, with third-country FIUs, having regard to Union law and to the principles relating to information exchange

340 Article 13 AMLD4.
341 Article 33 AMLD4.
342 Article 32 AMLD4.
343 Article 52 AMLD4.
344 Article 58 AMLD4.
345 Article 30 AMLD4.
346 Preamble 14 AMLD4.
347 Article 18 AMLD4.
348 Article 26, 2 AMLD4.

developed by the Egmont Group, *i.e.* an informal network of FIUs for the stimulation of international co-operation.[349]

4.2.3. Cryptocurrencies under AMLD4

Are transactions in cryptocurrencies included in the scope of AMLD4? Although there is some scholarly debate on this[350], it is fair to say that it is very difficult, if not impossible, to stretch the scope of AMLD4 so far as to include cryptocurrency transactions.[351]

A surmountable hurdle for cryptocurrencies to be included in the scope of AMLD4 is the connecting factor "*property*" or "*funds*". As aforementioned, property – and arguably, funds – Is defined as assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets. Although not written for cryptocurrencies, at first glance, this definition is broad enough to also include cryptocurrencies, as they could be seen as incorporeal immovable assets for the purposes of AMLD4.[352]

An insurmountable hurdle, however, is that of the list of obliged entities. None of the players in the cryptocurrency scheme, regardless of which cryptocurrency is concerned, is directly or indirectly included in the list of obliges entities, not even crypto exchanges. Therefore, the AMLD4 framework simply cannot be attached to the crypto scheme, exempting it fully from the AMLD4 scope.

This also came to the attention of the European Commission in 2016, which initiated legislative action to bring virtual currency exchange platforms and custodian wallet providers under the scope of the AMLD in the future.[353] The coming of age of this inclusion into the AMLD framework will be elaborated hereinafter. It is not the intention to discuss all steps that were taken, but only to highlight the important steps, ultimately with the aim to create a better understanding of where the final results and policy choices came from.

4.2.4. The coming of age of the inclusion of cryptocurrencies into AMLD5[354]

a. Preliminary remark: the terminology

Prior to deep diving into the coming of age of the inclusion of cryptocurrencies into AMLD5, we note that most of the policy documentation uses the term "virtual currencies" instead of cryptocurrencies. Important for this research is that cryptocurrencies are a subcategory of virtual currencies, more particularly that kind of virtual currencies that have a bi-directional link to the real economy. Therefore, when throughout this analysis of the regulatory framework we refer to virtual currencies, this includes cryptocurrencies. Moreover, when we look at the exact scope of the definitions included in the various policy documentation, there is a clear tendency towards targeting cryptocurrencies

---

[349] AMLD5 provides for additional measures, such as a requirement for Member States to refuse the establishment of subsidiaries or branches or representative offices of obliged entities from a high risk third country or prohibit obliged entities from establishing branches or representative offices in such a country (new Article 18a).

[350] It has e.g. been argued that crypto-exchanges and platforms that exchange 'virtual currency' into fiat money could fall within the definition of 'financial institutions' as set out in article 3(2)(a) of AMLD4, as this definition also includes the activities of "currency exchange offices" (see: C. HAUBEN, "Bitcoin en EU-recht: de virtuele vreemde eend in de bijt" in M. E. STORME and F. HELSEN (eds.), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia , 2017, 87), though this reasoning is not generally accepted.

[351] Very clearly: N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 286, 298-303 and 309.

[352] N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 295.

[353] See hereinafter: the road to AMLD5 for cryptocurrencies.

[354] See very informative http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml).

with these definitions andnot or only to a lesser extent other kinds of virtual currencies that have only a one directional or no link to the real economy.

b. The 2014 EBA opinion on virtual currencies

A first important step towards including the cryptocurrency scheme into the AMLD framework, is an opinion of the European Banking Authority in 2014 on virtual currencies.[355]

In this report the EBA advocates a comprehensive regulatory approach towards virtual currencies over time.[356] Preferably this is done through designing a tailored regulatory regime along the lines of the following characteristics: creating a virtual currency scheme governance authority that is accountable to the regulator, customer due diligence requirements, fitness and probity standards for individuals performing specified functions in a scheme governance body, exchange or other relevant market participants, mandatory incorporation in an EU Member State, transparent price formation and requirements against market abuse, authorisation and corporate governance requirements, capital requirements, evidence of secure IT systems, payment guarantee and refunds requirements, separation of virtual currency schemes from conventional payment systems and a global regulatory approach.

As a more immediate response, the EBA recommends to include market participants at the direct interface between conventional and virtual currencies, such as virtual currency exchanges, in the scope of the AMLD as 'obliged entities' and thus subject these to anti-money laundering and counter-terrorist financing requirements.

According to the EBA, this immediate response will 'shield' regulated financial services from virtual currency schemes, and will mitigate those risks that arise from the interaction between virtual currency schemes and regulated financial services. Other things being equal, this immediate response, according to the EBA, will allow virtual currency schemes to innovate and develop outside of the financial services sector, including the development of solutions that would satisfy regulatory demands on the longer term.

None of these options were eventually retained by the European legislator: no tailored framework was developed for virtual currencies, nor were the EBA's suggestions to expand the scope of the AMLD followed in the course of the - then ongoing - revision that led to the AMLD4.

c. The Council Invite

The momentum changed after the terrorist attacks in France. In meetings held in December 2015, the European Council concluded that rapid further action against terrorist finance was required. Following up on this, the Council on 12 February 2016 underlined the importance of achieving rapid progress on legislative actions identified by the Commission, including in the field of virtual currencies.[357] Therefore, it called upon the Commission to submit targeted amendments to AMLD4 and if necessary to the revised Directive on Payment Services ("***PSD2***") and to the Cash Control Regulation.

---

[355] EBA, "EBA Opinion on 'virtual currencies'", 4 July 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

[356] See below.

[357] Council conclusions on the fight against the financing of terrorism, 12 February 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/02/12/conclusions-terrorism-financing/.

d. The Commission's Supranational Risk Assessment

On 26 June 2017, the European Commission released its report on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (also referred to as the "***Supranational Risk Assessment***").[358] In its report the Commission identified virtual currencies as potentially vulnerable to money laundering and terrorist financing risks affecting the internal market. More in general, the Commission rightly identifies anonymity in financial transactions as a vulnerability common to all sectors, including the anonymity related to virtual currencies. Their anonymity features place an intrinsic limitation on identification and monitoring possibilities. The Commission goes as far as recommending Member States to extend already the list of obliged entities in the application of Article 4 of the AMLD4 and to consider including at least virtual currency exchange platforms and wallet providers in AMLD4's scope.

e. The Commission's Impact Assessment accompanying the AMLD5 proposal

In the build-up to a legislative proposal to amend the AMLD4, the Commission conducted an extensive impact assessment ("***Impact Assessment***")[359]. The Impact Assessment acknowledges the problem that suspicious transactions made through virtual currencies are not sufficiently monitored by the authorities, which are unable to link identities and transactions, mainly because of the anonymity surrounding virtual currencies and because of virtual currency schemes and their participants (users (traders, suppliers, customers), 'miners', currency exchange platforms, wallet providers, …) not being regulated.

Particularly interesting are the potential regulatory answers to address this problem. According to the Impact Assessment, these are the following.

i. First option: target users, including consumers and retailers using virtual currencies as an investment product or as a means of exchange for buying/selling products or services.

The Impact Assessment sees two ways to lift the anonymity of users. The first one is through the mandatory registration of users (option A). The second one is softer and reduces virtual currencies' anonymity through the voluntary self-registration of users (option B). This option would not eradicate anonymity, but would allow authorities combating financial crime to rapidly verify identities of registered users.

ii. Second option: target virtual currency exchange platforms

Again, the Impact Assessment suggests two ways forward. The first one is to make exchange platforms obliged entities under AMLD4 (option C), submitting them *inter alia* to customer due diligence requirements. The second way forward is to bring virtual currency exchange platforms under the scope of PSD2 (option D). PSD2 goes further than AMLD4. On top of the anti-money laundering and counter-terrorist financing requirements which it automatically imposes by reference

---

[358] ECOM(2017) 340 final. The Supranational Risk Assessment ("SNRA") was the final product of a review by the Commission of anti-money laundering and terrorist financing risks at Union level in the application of Article 6 of AMLD4. The SNRA was accompanied by an elaborate Commission Staff Working Document in which among others the money laundering and terrorist financing risks relating to virtual currencies are detailed (SWD(2017) 241 final). On the one hand, the risk levels relating to virtual currencies in the context of money laundering and terrorist financing are estimated moderately significant, which is a level 2 risk on a scale of 1 (low) to 4 (high risk): while terrorists or other criminals may have a high intent to use virtual currencies' due to their characteristics (anonymity in particular), the level of capability is lower due to high technology required. On the other hand, virtual currency schemes are assessed to be highly vulnerable for terrorist financing and money laundering, because they are not regulated in the EU.

[359] COMMISSION STAFF WORKING DOCUMENT 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/2016/0223 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN.

to AMLD4, PSD2 also establishes a licensing obligation for regulated entities, minimum capital requirements, safeguarding requirements, and consumer protection rules. This way forward is, hence, more burdensome for exchanges.

iii. Third option: target custodian wallet providers

As for the first and second option, the Impact Assessment suggests two possible actions, which are similar to the approaches suggested for exchange providers, hence: respectively bringing them under the scope of AMLD4 (option E) or under the scope of PSD2 (option F).

Why are only custodian wallet providers targeted? The *rationale* of the Impact Assessment is that software wallet providers only provide applications or programs running on users' hardware to access public information from a distributed ledger and access the network. Therefore, they are only a technical service provider. Custodian wallet providers on the contrary have custody over the user's public and private key, making them from a conceptual perspective quite similar to financial institutions holding bank or payment accounts. Therefore, they warrant more regulatory attention.

iv. Evaluation of the options

Having consulted relevant stakeholders, the Impact Assessment evaluates that there is a need to have gatekeepers that manage the control of users' identities when needed. In that respect, an overwhelming majority of Member States favoured option C over D, hence make virtual currency exchange platforms obliged entities under AMLD4 instead of including them in the scope of PSD2.[360] The options envisaging custodian wallet providers were apparently not in scope of the debate with the stakeholders, although some Member States nevertheless expressed a preference to include these in the scope of AMLD4, instead of in the scope of PSD2. Generally, any option involving PSD2 was thus not welcomed by most Member States. They believed that this would give too much legitimacy to virtual currencies and drive consumers to believe virtual currencies are safe and sound products, which they are not, according to the various warnings financial supervisors all across the globe have issued.

The virtual currency industry itself appeared to be generally favourable to legislation for two reasons: it would give them more legitimacy and it would help to differentiate between bona-fide users and criminals.

The options involving registration of users were apparently only tested with some relevant stakeholders (i.e. consumers/users, experts), resulting in a preference for non-mandatory registration.

f. The Commission's AMLD5 Proposal

In its proposed fifth revision of the AMLD ("***Commission Proposal***")[361], launched on 5 July 2016, the Commission eventually takes the approach of including both virtual currency exchanges (defined as "*providers engaged primarily and professionally in exchange services between virtual currencies and fiat currencies*") and custodian wallet providers (defined as "*wallet providers offering custodian services of credentials necessary to access virtual currencies*") in the scope of the AMLD and to label these as obliged entities. Consequently, going forward these entities will have to apply customer due

[360] All Member States were consulted and 27 supported option C with one exception having a preference for option D. Option E was also envisaged by some Member States even though not presented in the questionnaire.

[361] COM/2016/0450, "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", 6 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&qid=1523358551244&from=EN.

diligence controls when exchanging virtual for fiat currencies, ending the anonymity associated with such exchanges and such wallet providers, and report suspicious transactions to the competent FIU. In addition, virtual currency exchanges and custodian wallet providers will need to be licensed or registered; apparently the Commission leaves the option between licensing and registration open.

For legal certainty reasons, the Commission also proposes a definition of the term "*virtual currency*": "*a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*".

As regards user registration, the Commission takes no immediate action. Instead, it commits itself to including in its next supranational risk assessment, which is due by 26 June 2019, if necessary, appropriate proposals, including, where appropriate, with respect to virtual currencies, empowerments to set-up and maintain a central database registering users' identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users.

This does, however, not mean that users remain completely out of scope of the Commission Proposal. More in particular, users are targeted indirectly insofar they hold their virtual currencies via a custodian wallet provider or enter into virtual currency transactions via a virtual currency exchange platform. These users can no longer be anonymous, because of the customer due diligence requirements vested upon the custodian wallet provides and virtual currency exchange platforms.[362] All other users remain out of scope (for now).

g. The updated EBA Opinion

Following the Commission Proposal, the EBA published an update of its 2014 opinion on virtual currencies. The EBA welcomes this proposal as an important step to mitigate some of the financial crime risks arising from the use of virtual currencies. The EBA furthermore endorses the Commission's approach not to include virtual currency transactions in the scope of PSD2 for the time being, given the short time frame within which the Commission was asked to develop its proposals. Including such transactions within the scope of PSD2 requires further legal and business model analysis, the EBA opines. Moreover, the EBA seems to still favour a separate and tailored regulatory regime, the elements of which it proposed in its 2014 Opinion. To that end, the EBA invites the Commission to initiate as soon as possible the comprehensive analysis that is needed for assessing which, if any, regulatory regime would be most suitable for virtual currency transactions.

h. The 2016 ECB opinion on the Commission's proposal

In addition to the EBA, also the ECB, on 12 October 2016, released a report on the Commission Proposal.[363] In that report the ECB strongly supports including virtual currency exchange platforms and custodian wallet providers into the list of obliged entities, as well requiring them to be licensed or registered. The ECB, however, also expresses some concerns, under which that, while it is appropriate to regulate virtual currencies for combating money laundering and terrorist financing, regulation should not seek to promote a wider use of virtual currencies. Furthermore, the ECB makes technical comments relating to the definition of virtual currencies, that were later picked up in the compromise text, discussed hereinafter[364].

---

[362] N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 304.

[363] Opinion of the ECB of 12 October 2016 on a 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, https://www.ecb.europa.eu/ecb/legal/pdf/con_2016_49_with_technical_working_document_.pdf.

[364] See below.

i. Discussion in in Parliament

The Commission Proposal was thoroughly studied by members of the European Parliament throughout 2016 and 2017. An extensive report was adopted suggesting several amendments.[365] Particularly interesting are the suggestions made by the Committee on Legal Affairs of 18 January 2017. The Committee proposes to expand the scope of AMLD significantly as regards virtual currencies, so as to include virtual currency exchange platforms, custodian wallet providers, issuers, administrators, intermediaries and distributors of virtual currencies, and administrators and providers of systems for online payments. This is very broad and potentially brings all virtual currency service providers under the AMLD's scope. This has been criticized by some legal doctrine to the extent the scope also includes purely technical service providers, such as miners of cryptocurrencies, or is simply not realistic, because there is no central issuer – as is the case for many cryptocurrencies.[366]

Furthermore, the Committee on Legal Affairs is of the opinion that to combat the risks related to anonymity, national FIUs should be able to associate virtual currency addresses to the identity of the owner of virtual currencies.

The scope extensions were not picked up in the Compromise Text, which is analyzed hereinafter.

j. The Compromise Text

On 13 December 2017, and following the technical work thereafter, a provisional agreement was reached between the Parliament and the Council on AMLD5, which resulted in a final compromise.[367] This was formally adopted by the European Parliament in plenary on 19 April 2018.[368] On 14 May 2018, the Council approved the European Parliament's position at first reading.[369] AMLD5 will enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.[370] Member States will have to bring into force laws, regulations and administrative provisions necessary to comply with AMLD5 by 10 January 2020.

Overall, the adopted Compromise Text is in line with the Commission Proposal. Nevertheless, there are some differences.

Firstly, the Compromise Text uses different wording to include virtual currency exchange services and custodian wallet providers in the list of obliged entities (the changes compared to the Commission Proposal are marked hereinafter: "providers engaged[371] in exchange services between virtual currencies and fiat currencies and custodian wallet providers"[372].

---

365 EP Report 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, 9 March 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN#title1.

366 N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 293.

367 See: http://data.consilium.europa.eu/doc/document/ST-15849-2017-INIT/en/pdf.

368 European Parliament legislative resolution of 19 April 2018 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)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0178+0+DOC+PDF+V0//EN.

369 See: https://eur-lex.europa.eu/procedure/EN/2016_208.

370 AMLD5 was published in the Official Journal of the European Union on 19 June 2018. See: Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, *OJ L* 156, 19 June 2018, 43 (electronically available via: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN).

371 Hence, the qualifier of "primarily and professionally" was dropped, meaning that also those providing these services occasionally would be caught under the scope. Vandezande raises the question of whether a virtual currency user, who on a non-commercial basis – for instance as a gesture to a friend – exchanges some units of virtual currency for legal tender or similar instruments, could become an

Secondly, the Compromise Text uses a slightly different definition of virtual currencies. More in particular, it defines virtual currencies as "*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically*" (the changes compared to the Commission Proposal are marked hereinafter: "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically").

Thirdly, a definition of "custodian wallet provider" ("an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies") is included. Such a definition was not included in the Commission Proposal.

Fourthly, the Compromise Text is more precise on whether exchange platforms and custodian wallet providers should be licensed or registered: they should be registered (the changes compared to the Commission Proposal are marked hereinafter: "ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered").

The obligation for the Commission to assess the desirability of a (voluntary) registration of users in the course of its next supranational risk assessment, due by 26 June 2019, is unchanged.

4.2.5. Funds Transfer Regulation

As aforementioned, the anti-money laundering framework as introduced in 2015 also includes the Funds Transfer Regulation or FTR. It is interesting to see whether this regulation somehow is a useful instrument to combat the illicit use of cryptocurrencies.

The FTR lays down rules on the information on payers[373] and payees[374] accompanying transfers of funds, in any currency, for the purposes of preventing, detecting and investigating money laundering and terrorist financing (as defined under AMLD4), where at least one of the payment service providers[375] involved in the transfer of funds is established in the Union. Particularly, the FTR requires the payment service provider of the payer to ensure that transfers of funds are accompanied by the name of the payer, the payer's payment account number, the payer's address, official personal document number, customer identification number or date and place of birth, the name of the payee and the payee's payment account number[376], absent which he cannot execute any transfer of funds.[377] The payment service provider of the payee is required to detect missing information on the

obliged entity under the anti-money laundering framework: N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 292.

372 The proposed Preamble 7a elaborates on the difference with e-money: virtual currencies should not to be confused with electronic money as defined in the e-money Directive nor with the larger concept of "funds" as defined in point (25) of Article 4 of PSD2 nor with monetary value stored on instruments exempted as specified in Article 3(k) and 3(l) of PSD2, nor with in-games currencies, that can be used exclusively within the specific game environment. Whilst they could frequently be used as a means of payment, they may also be used for other different purposes and find broader applications such as means of exchange, investment purposes, store-of-value products or uses in online casinos. The objective of AMLD5, the Preamble continues, is to cover all the potential uses of virtual currencies. The exact added value of this Preamble is not very clear.

373 "Payer" means a person that holds a payment account and allows a transfer of funds from that payment account, or, where there is no payment account, that gives a transfer of funds order (Article 3, (3) FTR).

374 "Payee' means a person that is the intended recipient of the transfer of funds (Article 3, (3) FTR).

375 "Payment service provider" means *inter alia* the categories of payment service providers referred to in Article 1(1) of the former Payment Services Directive (Article 3, (5) FTR).

376 Article 4, 1 and 2 FTR.

377 Article 4(6) FTR.

payer or the payee.[378] Where the payment service provider of the payee becomes aware of missing or incomplete information, he must reject the transfer or ask for additional information.[379] Furthermore, he is required to take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported to the competent FIU in accordance with AMLD4.

With some exceptions, the FTR applies to transfers of funds[380], in any currency, which are sent or received by a payment service provider or an intermediary payment service provider established in the EU.[381] "Funds" means banknotes and coins, scriptural money and electronic money.[382]

Here's the rub: cryptocurrencies are none of those, and, hence out of scope. Moreover, crypto intermediaries as a rule will not be payment service providers or intermediate payment service providers in the meaning of the FTR[383]. This is a second reason why the FTR is not equipped to fight the illicit use of cryptocurrencies, apart from it not being designed with cryptocurrencies in mind, which is apparent from the information to be provided, especially the reference to account numbers.

4.2.6. Cash Control Regulation

As an add-on to its money laundering and terrorist financing framework, the EU enacted already in 2005 rules on the control of cash entering or leaving the Union.[384] These rules intend to address cash movements for illicit purposes. They apply to significant movements of cash crossing the borders of the Union, i.e. cash movements equal to or above EUR 10.000 by any natural person entering or leaving the Union. Such a person must declare the cash movement, enabling customs authorities to gather information on the movements and, where appropriate, transmit that information to other authorities.

In the context of the Cash Control Regulation, "*cash*" means: (a) bearer-negotiable instruments including monetary instruments in bearer form such as travellers cheques, negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery and incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted; and (b) currency (banknotes and coins that are in circulation as a medium of exchange).[385]

Can cryptocurrencies be included in this definition? Remarkably, theoretically, there is an opening. Coins that are in circulation as a medium of exchange are in scope. Cryptocurrencies can be seen as such coins, which is also evidenced by the AMLD5 definition of virtual currencies.

---

[378] Article 7 FTR.

[379] Article 8 FTR.

[380] "Transfer of funds" means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same (Article 3, (9(FTR).

[381] Article 2 FTR. Please note that the regulation also has EEA relevance.

[382] Article 3, (8) FTR.

[383] Also see the similar reasoning why crypto intermediaries are thought not to be in scope of the PSD2.

[384] Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, *OJ L* 309, 25 November 2005, 9 (electronically available via: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R1889&from=EN).

[385] The current 2005 framework is currently under revision and will be replaced by a new one, taking into account the development of new best practices in the implementation within the EU of international standards on combating money laundering and terrorism financing developed by the FATF (https://ec.europa.eu/taxation_customs/sites/taxation/files/com_2016_825_en.pdf). The proposed new framework extends the definition of cash to some instruments or methods of payment other than currency, such as cheques, traveller's cheques, gold and prepaid cards.

Nonetheless, it is clear that the Cash Control Regulation is not written with movements of cryptocurrencies in mind. It is written with physical movements of cash in mind, explaining *inter alia* the requirement to declare and the involvement of customs authorities. Cryptocurrencies are normally not moved physically: when they move, they move digitally. This makes the cash control framework intrinsically unfit to track movements of cryptocurrencies. From a practical perspective, a scholarly debate on the inclusion of cryptocurrencies into the scope of the Cash Control Regulation, therefore, is not very useful. The one event wherein it could be of any use is when cryptocurrencies would be stored onto a portable carrier, such as an USB-stick, making that stick some sort of a bearer instrument, and this stick would be moved across the EU border. But even for this event, it does not help a lot to include it into the scope of the Cash Control Regulation. After all, even leaving aside issues of proportionality and data protection, it seems not very practical – and desirable – to verify the content of every USB-stick or the like moving across Union borders.

4.3. Tax evasion

The second part of this research's analysis of the regulatory framework relates to tax evasion.

As was already explained above[386], the EU framework that is in place on the exchange of information in tax matters, specifically aiming at combating tax evasion, is not very well equipped to address the use of virtual currencies for tax evasion, because to be able to share information on this, authorities must have the information in the first place, which is being complicated, if not made impossible, by the anonymity surrounding cryptocurrencies.

Salvation could lie in the anti-money laundering and counter-terrorist financing framework. To the extent this framework unveils anonymity, the relevant information is registered into a central database *and* the tax authorities are able to consult and use this information, the fight against tax evasion through cryptocurrency transactions could become more effective.

Is this something that can be done already under the current AMLD framework?

Firstly, it can be noted that the definition of "criminal activity" under AMLD4 includes tax crimes relating to direct taxes and indirect taxes, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year.[387] Hence, the use of illegal proceeds of tax crimes is in scope of AMLD4 and can constitute money laundering. Therefore, obliged entities who know, suspect or have reasonable grounds to suspect that proceeds stem from tax evasion must inform the competent FIU. The FIU will analyse the file and disseminate the results of its analysis to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing. When it relates to a cross-border file the FIUs concerned have to cooperate and exchange the obtained information with each other to the greatest extent possible. In this respect, the AMLD4 imposes that differences between national law definitions of tax crimes can be no impediment to the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law.[388]

In the context of all this, FIUs and competent authorities should have access to the beneficial ownership register, allowing them to verify beneficial ownership of corporate and other legal entities.

---

386 See: setting the scene.

387 Article 3, (4)(f) AMLD4 and Preamble 11 AMLD4.

388 Article 57 AMLD4. In addition, according to Preamble 56 of the AMLD4, the exchange of information on cases identified by FIUs as possibly involving tax crimes should be without prejudice to the exchange of information in the field of taxation in accordance with Directive 2011/16 or in accordance with international standards on the exchange of information and administrative cooperation in tax matters. As aforementioned, the latter directive does not help out a lot currently as regards fighting tax evasion via the use of cryptocurrencies.

This can be very helpful when these corporates or other legal entities are in fact set-up to mask their beneficial owners for purposes of tax evasion. Other persons than competent authorities and FIUs who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as tax crimes, will also be granted access to beneficial ownership information, in accordance with data protection rules, as already aforementioned.[389]

Is the tax administration a competent authority who can get access to the beneficial ownership register? There is no definition of what constitutes a "*competent authority*" under AMLD4, basically leaving it open for Member States to decide who the competent authorities within their respective territories are. At least theoretically, this could mean that the tax administration is not a competent authority. What is clear, however, is that within each Member State a competent authority should be able to initiate administrative or criminal proceedings against launderers of proceeds of tax crimes. If not, that would probably be in breach of Article 58, 2 of AMLD4, requiring Member States to have in place and make available to competent authorities a sanctioning toolbox allowing them to adequately sanction breaches of the national provisions transposing AMLD4.

However it may be, the fifth revision of the Directive on administrative cooperation in taxation in 2016 ("**DAC5**") took away all doubt: as of 1 January 2018 tax authorities must have access to the information gathered in the context of combating money laundering and terrorist financing, including the beneficial ownership register.[390]

AMLD5 acknowledges this established right.[391] It explicitly lists tax authorities in the list of competent authorities that must be granted access to the beneficial ownership register.[392] The tax administration is also explicitly recognized in Article 49 of the revised AMLD framework, requiring Member States to ensure that tax authorities when acting within the scope of the AMLD, have effective mechanisms to enable them to cooperate and coordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing. In this context, it is furthermore made clear that a request for assistance between competent authorities cannot be refused on the grounds that the request is also considered to involve tax matters.[393]

All these innovations brought by DAC5 and AMLD5 strengthen the tax authorities' toolbox to pick up the gauntlet against tax evasion, in addition to other competent authorities that may also have sanctioning powers in this field, such as public prosecutors.

The above analysis is a general one. What does all of it mean for tax evasion through the use of cryptocurrencies? Well, under AMLD4 cryptocurrencies are not in scope because none of the crypto

---

389 Preamble 14 AMLD4.

390 Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, *OJ L* 342, 16 December 2016, 1 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2258&from=EN).

391 As a side note, we mention that a similar clarification of the right to access information by tax authorities is recently also envisaged in a pending proposal for a directive laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences (COM (2018) 213), which is perceived as an add-on to the AMLD framework. This directive relates to financial information and bank account information contained in the centralised bank account registries. "Financial information" is defined rather broadly as any type of information or data which is held by FIUs to prevent, detect and effectively combat money laundering and terrorist financing, or any type of information or data which is held by public authorities or by obliged entities for those purposes and which is available to FIU without the taking of coercive measures under national law. This could be information relating to cryptocurrencies, so it seems. What is remarkable, however, is that nonetheless the proposed Preamble 9 is clear about the tax authorities' rights to information, the proposed text of the directive itself, particularly Article 3, is a lot less clear about this.

392 Amended Articles 30 and 31 AMLD.

393 Article 50a of the revised AMLD.

players are obliged entities, as analysed already above. So, there is no information available within the AMLD framework to be accessed by the tax administration. Thus, this is not much of a help.

Under AMLD5, virtual currency exchange platforms and custodian wallet providers become obliged entities and cryptocurrencies - via the concept "*virtual currencies*" - are brought in scope. So, insofar cryptocurrency is held through a custodian wallet provider or transactions occur via a virtual currency exchange platform, there will be information available for the tax administration, as the case may be brought to the attention of the tax administration by an FIU reporting a suspicious transaction linked to tax evasion.

5. ADEQUACY OF THE REGULATORY FRAMEWORK

5.1. Introduction

Now that we have a clear picture of the current and upcoming regulatory framework for combating money laundering, terrorist financing and tax evasion via cryptocurrencies, it is high time to analyse whether that framework is adequate to address the many challenges cryptocurrencies bring.

The existing framework is not adequate. This we have already analysed above.

How does the upcoming AMLD5 score and what would be a good way forward?

We will hereinafter try to answer that question on the basis of a number of more technical sub-questions[394]. The questions are the following.

- Is the definition of virtual currencies sufficient to capture the cryptocurrencies that can be used to launder money, finance terrorists or evade taxes?
- Is it enough to include only custodian wallet providers and virtual currency exchanges in the list of obliged entities?
- Does the AMLD5 framework allow to pull enough cryptocurrency users into the light?
- Would it make sense to extend the scope of the Funds Transfer Regulation and/or the Cash Control Regulation as to include cryptocurrency transactions?
- Is there a need for a more comprehensive approach, introducing license requirements for cryptocurrency players?
- Is it not best to outright ban some activities or aspects linked to cryptocurrencies?
- Is the European level the appropriate level to tackle money laundering, terrorist financing and tax evasion via cryptocurrency transactions?

It is not our intention to give the definitive answer to all the questions raised. What we do intend is to give our analysis and to fuel the further debate.

5.2. Is the definition of virtual currencies under AMLD5 sufficient?

As a recall, the definition of virtual currencies under AMLD5 is the following: "*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically*".

5.2.1. Conclusions on the basis of the taxonomy

Referring back to our taxonomy of cryptocurrencies, we can conclude that almost all of the cryptocurrencies scrutinized fit within this definition. All of the cryptocurrencies are:

- a digital representation of value;
- decentralized, *i.e.* not issued or guaranteed by a central bank or a public authority;
- not attached to a legally established currency;

[394] It is not our intention to give a comprehensive list of all the relevant sub-questions instrumental to assessing the framework's adequacy. The selected questions allow to draw some preliminary conclusions though.

- not possessing the legal status of currency or money;
- electronically transferable, storable and tradeable.

The one element that could give rise to discussion is that of the cryptocurrencies having to be a means of exchange. The AMLD5 does not provide further guidance of what this means, but an acceptable interpretation is that the cryptocurrencies should be able to be used to facilitate the sale, purchase of trade of goods between parties and represent a standard of value that is accepted between the parties.[395]

Two questions arise.

Firstly, what if a cryptocurrency is not accepted as a means of exchange now, but there is no intrinsic limitation preventing it from becoming a means of exchange in the future? This is for instance relevant for cryptocurrencies that are apparently not used as a means of exchange now, such as IOTA and NEO. But that may change. All depends on the willingness of parties to accept the cryptocurrency as a standard of value in their mutual dealings. As soon as that happens, they become a means of exchange and tumble into the scope of the definition of "virtual currencies" under AMLD5. Therefore, from the perspective of combating money laundering, terrorist financing and tax evasion, there is no big issue: normally, committing one of these offences via cryptocurrencies implies having done an exchange, implying the cryptocurrency used is a means of exchange and is included in the scope of AMLD5.

Secondly, what if a cryptocurrency is a medium of exchange, but also and foremost an investment instrument? This is an extremely relevant question, as it is very clear from high volatility and various warnings from financial supervisors that some cryptocurrencies are considered an investment instrument by users, not in the least Bitcoin, which still has the highest market capitalisation of all cryptocurrencies. If the answer to this question would be that these cryptocurrencies are out of scope, this would mean that AMLD5's fruits all in all are very little. We argue against such an interpretation. AMLD5's definition requires cryptocurrencies to be accepted as a means of exchange. It does not say that this should be the only or predominant function of the cryptocurrency. Therefore, it does not matter if the cryptocurrency is also or predominantly an investment instrument. Also in that event, the cryptocurrency is included in the scope of AMLD5. Furthermore, an argument can be derived from the fiat currency framework: a fiat currency can also be acquired and held for investment (speculation) purposes; this does not change the fiat currency's primary status of being a fiat currency.

Therefore, we conclude that AMLD5's definition of virtual currencies is sufficient to combat money laundering, terrorist financing and tax evasion via the cryptocurrencies included in our taxonomy. Of course, that taxonomy is not exhaustive. Nevertheless, we believe that it is fairly representative for the cryptocurrencies that are out there, both from the perspective of market capitalisation and from the perspective of distinctive features. Therefore, we believe that our conclusion here, and the conclusions that follow below, should also be representative, although it cannot be ruled out that some conclusions may not or not to the same extent apply to cryptocurrencies that were not in scope of this research.

5.2.2. Other virtual currencies than cryptocurrencies

Virtual currencies within the scope of AMLD5 are those that can be transferred, stored and traded electronically. There is no requirement that virtual currencies are bi-directionally transferable or

[395] See: https://www.investopedia.com/terms/m/mediumofexchange.asp.

tradeable against fiat currencies. This means, for instance, that virtual currencies that can be acquired with fiat money and then used only in the virtual world to buy goods or services and/or that are transferable or tradeable only against other virtual currencies, are also included in the scope of the AMLD5 definition of virtual currencies.

However, legal doctrine rightly analysed that this inclusion in the scope of AMLD5's definition of virtual currencies does not help a lot looking at the list of obliged entities.[396] The analysis is that the list of obliged entities, and especially the reference to virtual currency exchanges as defined by AMLD5, shows that the scope of the anti-money laundering regulation of virtual currencies is limited to certain bi-directional scheme virtual currencies only. Other virtual currency schemes are not in scope, including virtual currency to virtual currency exchanges and virtual currencies used to attain goods and services without requiring exchange into legal tender or similar instruments, or the use of a custodian wallet provider[397]. This leaves a blind spot, allowing such activities to still result in money laundering or terrorist financing activities outside of the scope of AMLD5.

Is it a problem? Well, yes and no.

No, because it is arguable that some types of virtual currencies are of minor to no importance for money laundering or terrorist financing, for instance virtual currencies that can only be obtained and used in the virtual world and have no interaction with the real economy. This makes them not very useful for money laundering or terrorist financing purposes. Schemes allowing to acquire virtual currencies with fiat currency, but where the acquired virtual currency can only be used in the virtual environment suffer the same defect for purposes of money laundering or terrorist financing, given that no money can flow out of the system. Of course, it is possible that in such a scheme the acquired virtual currency can be used as a means of payment (e.g. when a person consents to receiving payment in virtual currency). Nevertheless, it is assessed that such a method is fairly unsuited for larger scale money laundering operations.[398] Therefore, arguably predominantly the schemes allowing to acquire virtual currency against fiat money and allowing to sell virtual currency against fiat money pose the biggest threat, as they can be linked to cash both at the entry into and the exit from the virtual sphere.

Yes, because the world of cryptocurrencies is a fast moving one and the network of acceptance of virtual currencies can grow, the Impact Assessment rightfully points out. If virtual currencies effectively become widely accepted and used, there might come a point in time when there will no longer be a need to convert virtual currencies back into fiat currencies. In other words, with a growing network of acceptance, the need to "cash-out" of virtual currencies and exchange them for fiat currencies might decrease over time. This trend would, according to the Impact Assessment, increase further if virtual currencies would become less volatile.

Therefore, it is important to closely follow-up and monitor the use cases of virtual currencies, and especially whether the use of virtual currencies within a virtual setting and without having to cash-out again becomes increasingly important.[399] When that would actually happen, the regulatory framework should follow and include these cases into its scope. Or, as the IMF points out more

---

396 N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 303.

397 *Ibid.*

398 N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 278-279.

399 Also see the IMF's advice: IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 37.

broadly, the changing nature of the technology requires that regulation be flexible and can be adapted to evolving circumstances.[400]

5.3. Is it enough to include only custodian wallet providers and virtual currency exchanges in the list of obliged entities?

5.3.1. State of play

We recall AMLD5's definitions of custodian wallet providers and virtual currency exchanges. These are respectively: "*an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies*" and "*providers engaged in exchange services between virtual currencies and fiat currencies*".

Above we have identified the key players in the cryptocurrency market: users, miners, cryptocurrency exchanges, trading platforms, wallet providers, coin inventors and offerors.

Clearly, a number of these key players are not obliged entities under AMLD5.

5.3.2. Users

Firstly, users are not obliged entities under AMLD5. Making them obliged entities would not make a lot of sense, as the AMLD framework for a large part focuses on intermediaries[401]. In any event, it would not be proportionate[402]. So, this is fine.

5.3.3. Miners

Secondly, miners are also not obliged entities. And, as for users and for the same reasons, at first glance making them obliged entities would probably make little sense. According to the Impact Assessment, there are mainly two reasons for not considering miners as obliged entities. Firstly, miners are considered to be more a sort of technical service providers than gatekeepers between the virtual sphere and the real world. Secondly, miners are mostly located in China which would make any initiative largely impossible to enforce.

Nevertheless, two critical observations can be made here. Firstly, miners can be cryptocurrency users too, or, more commonly, parties who have made a new business out of mining cryptocurrencies to sell them for fiat currency or for other cryptocurrencies.[403] Along the same lines it is not inconceivable that criminals start mining cryptocurrencies to do the same - if they are not already doing this.[404] Mining Bitcoins is probably hard to do for criminals, given that it requires massive server power and substantial knowhow, but the same is not necessarily true for other cryptocurrencies, which can be easier to mine and still from the own living room so to speak.[405] Once mined, the cryptocurrencies can be linked to the real world. Secondly, we are not sure that mining is done from China predominantly. This is true for Bitcoins and probably also for other major coins requiring a certain level of

---

[400] IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 26-27.

[401] It of course also includes rules on the beneficial ownership register. This can include info on cryptocurrency users to the extent these users are corporate or other legal entities.

[402] Also see on the US approach not to target users via regulation: T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, http://digitalcommons.law.msu.edu/jbsl, 182.

[403] At which time they become offerors; see hereinafter.

[404] See with respect to cryptocurrencies running on permissionless, public blockchains: J. BLUMBERG, "We Need To Shut Bitcoin And All Other Cryptocurrencies Down. Here's Why.", March 2018, https://www.forbes.com/sites/jasonbloomberg/2018/03/10/we-need-to-shut-bitcoin-and-all-other-cryptocurrencies-down-heres-why/#1dbed32b1bca.

[405] See e.g. https://cryptocurrencyfacts.com/asic-mining-basics/; https://www.coinwarz.com/cryptocurrency.

sophistication to mine, but is it also true for the cryptocurrencies that are easier to mine? Because criminals may be attracted to the mining business, some commentators even advocate a "know your miner" policy, at least with respect to the cryptocurrencies that run on permissioned blockchain technology (because for those that run on permissionless blockchain technology, it is hard to find out their identities)[406].

At present, the fact that the mining business is succeptible for illegitimate use, appears to be underestimated. Going forward, increasing attention should be devoted to the risks that accompany it, especially in light of the number of cryptocurrencies that is minable (i.e. based on a PoW consensus mechanism). The exclusion of miners from AMLD5's scope, currently leaves a blind spot in the EU's fight against money laundering, terrorist financing and tax evasion.

5.3.4. Cryptocurrency exchanges

Thirdly, we have identified cryptocurrency exchanges as relevant players. Most of these allow users to sell their cryptocurrency for fiat currency or buy new cryptocurrency with fiat currency. It is clear from the definition of virtual currency exchanges in AMLD5 that cryptocurrency exchanges of this nature are obliged entities.

However, there also pure cryptocurrency exchanges, only accepting payments in other cryptocurrencies, usually Bitcoin. Insofar as these exchanges do not also qualify as custodian wallet providers, they remain out of AMLD5's scope because they have no dealings with fiat currency. This is a blind spot in the fight against money laundering, terrorist financing and tax evasion, because it can add an extra layer of disguise of the origin of the cryptocurrencies (when they later pass through an obliged entity) or simply allow that cryptocurrencies are used completely outside of the monitored system.

The atomic swap, which in its essence is a pure cryptocurrency exchange 2.0, because it can function without the need of a third party, deserves special emphasis. As other pure cryptocurrency exchanges it is outside of the scope of the AMLD 5 and, thus, a blind spot. Contrary to other exchanges, it is also hard to bring it into the scope, because of the absence of a middleman. Therefore, if this over time would become a succesful platform through which criminals operate, it will be hard to find the right regulatory answer.

5.3.5. Trading platforms

As a fourth player, we identified trading platforms, which function as a market place bringing together different cryptocurrency users that are either looking to buy or sell cryptocurrencies and allow them to interact directly. Such trading platforms are so-called "P2P exchanges" or "decentralised exchanges" and differ from cryptocurrency exchanges in a number of ways, as elaborated above. For the purposes of attaching regulation to these trading platforms it is important that they are not run by an entity or company that oversees and processes all trades, but they are operated exclusively by software (*i.e.* there is no central point of authority). This simply makes it very hard to regulate them and *a fortiori* to include them in the list of obliged entities. Again, this is a blind spot in the fight against money laundering, terrorist financing and tax evasion, for the same reasons as aforementioned with respect to pure cryptocurrency exchanges.

[406] J. BLUMBERG, "We Need To Shut Bitcoin And All Other Cryptocurrencies Down. Here's Why.", March 2018, https://www.forbes.com/sites/jasonbloomberg/2018/03/10/we-need-to-shut-bitcoin-and-all-other-cryptocurrencies-down-heres-why/#1dbed32b1bca.

5.3.6. Wallet providers

Next, we identified wallet providers as key players. We made a distinction between three types:

- hardware wallet providers that provide cryptocurrency users with specific hardware solutions to privately store their cryptographic keys;
- software wallet providers that provide cryptocurrency users with software applications allowing them to access the network, send and receive cryptocurrencies and locally save their cryptographic keys; and
- custodian wallet providers that take (online) custody of a cryptocurrency user's cryptographic keys.

As aforementioned, only custodian wallet providers, defined as entities that provide services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies, are obliged entities under AMLD5. Hardware wallet providers and software wallet providers are not custodian wallet providers, as they do not safeguard keys on behalf of their customers, but merely provide the tools to customers to safeguard their cryptocurrencies themselves. So, again there is a blind spot in the fight against money laundering, terrorist financing and tax evasion. Users using software or hardware wallets escape AMLD5, as long as they also stay away from exchanges exchanging cryptocurrencies into fiat money.

5.3.7. Coin inventors

Sixthly, we identified coin inventors as key players. These were the individuals or organisations who have developed the technical foundations of a cryptocurrency and set the initial rules for its use. Often they remain unidentified, making them a hard category to target. On the other hand, it does not seem necessary to target them. As coin inventors, they are only the founding fathers of cryptocurrency schemes. They only provide the technological tools for others to work with. However, if and when they would take-up a different role, the situation might change. Depending on which role they take-up concretely they can then fall into one of the above categories or the below category.

5.3.8. Offerors

That brings us to the last category we identified: the offerors of cryptocurrencies, of course to the extent an offeror can be identified; some coins do not have an identifiable offeror. Coin offerors are individuals or organizations that offer coins to cryptocurrency users upon the coin's initial release, either against payment (i.e. through a crowd sale) or at no charge (i.e. in the framework of a specific (sign-up) program (e.g. Stellar)). When coins are offered this way, we speak of an initial coin offering in the true meaning of the word.[407]

Offerors are clearly not obliged entities under AMLD5. Moreover, they will most likely also not be caught by financial services laws, because it is difficult to include cryptocurrencies into the scope of these laws.[408] So, again, there is a blind spot in the fight against money laundering, terrorist financing and tax evasion.

[407] The terminology initial coin offering is often used as an umbrella term referring to all kinds of offerings, mostly of tokens. Here, it is used in its pure meaning: that of an offering of coins.

[408] See supra footnote 316. Going forward these offerors could be a useful connecting factor for financial services laws, if it would be decided to subject cryptocurrencies to financial services laws.

5.3.9. The initial question

Moving over to the initial question: is it enough to include only virtual currency exchanges and custodian wallet providers in the list of obliged entities under AMLD5?

What is certain is that there are relevant crypto players that are not caught by AMLD5[409], sometimes because the legislator chose not to (this is true for software wallet providers and pure cryptocurrency exchanges that are not custodian wallet providers), but, so it seems, sometimes also because he did not pay a lot of attention to their existence and the potential risks envolved (this is e.g. true for the trading platforms, that, admittedly, escape regulation anyway because there is no one to attach it to; for miners, hardware wallet providers and coin offerors). This leads to blind spots in the fight against money laundering, terrorist financing and tax evasion.[410]

Does it matter?

Maybe. It all depends on whether these blind spots are actually going to be exploited by criminals. Our estimation is that it would not be so surprising if persons with malicious intent would actually look up these blind spots in the shadow of AMLD5. If that would happen and it would appear to have a (material) adverse effect on the fight against money laundering, terrorist financing and tax evasion, there is definitely something to say for expanding the list of obliged entities with those players that were identified the weak spots or have great potential of being weak spots.[411] It is therefore important to closely follow-up on this and to intervene when required.

Meanwhile, an interesting thing is to watch is the emergence of self-regulation.[412] There have been reports of crypto players voluntarily applying customer due diligence to maintain a leading commercial edge over others.[413] If that would become a more general trend, it could very well influence the assessment of whether or not a hard law approach, via an amendment of the list of obliged entities, is necessary.

5.4. Does the AMLD5 framework allow to pull enough cryptocurrency users into the light?

This bring us to the next question in need for an answer: does the AMLD5 framework allow to pull enough cryptocurrency users into the light? This question boils down to finding out how anonymous their actions can still be on the crypto market after AMLD5.

First, and as already mentioned before, under AMLD5 users that hold their virtual currencies via a custodian wallet provider or enter into virtual currency transactions via a virtual exchange platform can no longer be anonymous, because of the customer due diligence requirements vested upon the custodian wallet providers and virtual currency exchange platforms.

---

409 Also see N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 308.

410 It is interesting to note that in the legislative process, as elaborated above, the suggestions made by the Committee on Legal Affairs of 18 January 2017 broadened the scope of the AMLD5, thus further limiting the blind spots. These suggestions were not picked up later on.

411 A different perspective is that of unfair competition. It has been argued that bringing some virtual currency service providers under the scope of the AMLD5, whereas others, who provide similar services, escape, fosters unfair competition: N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 309.

412 See also: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 55-56 (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

413 See for the US: T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, http://digitalcommons.law.msu.edu/jbsl, 215.

However, users using hardware or software wallets and for instance trade via a P2P network or via any other way than through a virtual currency exchange platform, can still operate anonymously.[414]

For those crypto players deliberately left out of the scope of AMLD5, the legislator is of course aware of this risk.[415] The solution proposed to address it is that national FIUs should be able to associate virtual currency addresses to the identity of the owner of virtual currencies and that the possibility for users to self-declare to designated authorities on a voluntary basis should be further assessed.

Concretely, however, as aforementioned, no immediate action is taken. The only achievement is a requirement for the Commission to include in its next supranational risk assessment, which is due by 26 June 2019, if necessary, appropriate proposals, including, where appropriate, with respect to virtual currencies, empowerments to set-up and maintain a central database registering users' identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users. This seems to point in the direction of a system of voluntary registration, instead of mandatory registration (which was also an option brought forward by the Impact Assessment), if at all any system will be retained following the next supranational risk assessment. Bearing in mind the timing of that assessment and that of potential subsequent AMLD amendments coming into force, it is clear that nothing is to be expected from Europe very soon.

This is a very soft approach towards unveiling anonymity of users and linking them to cryptocurrencies and cryptocurrency transactions. First, it is not sure that a system of registration will be introduced. Secondly, if ever a system would be put in place, it would be a voluntary one. It can very much be doubted if the category that should be targeted the most, users of cryptocurrencies for illicit purposes, would voluntarily register as a user. That would be like trusting the thief to come to the police station voluntarily after committing a theft. All in all, the approach taken is therefore not very convincing if the legislator is truly serious about unveiling anonymity of cryptocurrency users to make the combat against money laundering, terrorist financing and tax evasion more effective. A mandatory registration and a pre-set date as of which it applies, is to that end a much better approach, albeit of course more intrusive.

In this respect we also note that some cryptocurrencies that are now on the market, such as Dash and Monero, are fully anonymous, whereas others, such as Bitcoin and the like are pseudo-anonymous, basically meaning that if great effort is made and complex techniques are deployed, it is possible for authorities to find out users' identities. These fully anonymous cryptocurrencies are designed to stay in the dark and outside of the scope of authorities. After AMLD5 this will no longer be possible to the fullest extent: the cryptocurrency users that want to convert their cryptocurrency into fiat currency via a virtual currency exchange or hold their portfolio via a custodian wallet provider, will be subject to customer due diligence. But, as aforementioned, there is still a whole world outside of these new obliged entities under AMLD5. It goes without saying that this may sound particularly interesting for criminals seeking for new ways to launder money, finance terrorists or evade taxes. If a legislator does not want to outright ban these cryptocurrencies - and for not imposing such a ban a good argument is that cash is also fully anonymous and lawful - the only way to find out who uses them is to require users to register mandatorily. For reasons of proportionality it could then be considered to make the registration subject to a materiality threshold.

---

[414] See also: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 38-42 (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

[415] The legislator admits this explicitly in the Commission Proposal and the proposed Preamble 7 of the Compromise Text.

Of course, naivety is not in its place here. The adequacy of a mandatory registration of users, whether or not of fully anonymous or pseudo-anonymous cryptocurrencies, depends on the users' compliance with the registration requirement. Such compliance will partly depend on an adequate sanctioning toolbox in the event of breach, which is a necessity. But how do we detect a breach? Is this at all possible outside of the context of randomly bumping into it, at least when fully anonymous cryptocurrencies are concerned? This remains a loose end, even in a system of mandatory registration, and even when a ban would be imposed on technology fully anonymising cryptocurrencies, which will elaborated below.

An interesting line of thought here is again self-regulation: crypto intermediaries could decide for themselves not to accept fully anonymous cryptocurrencies in the course of their business. That could give them a reputational advantage over others, possibly also leading to a commercial advantage. If that would become a more general trend, it could have an influence on the assessment of whether or not a hard law approach, via registration of users, is necessary.

5.5. Would it make sense to extend the scope of the Funds Transfer Regulation and/or the Cash Control Regulation as to include cryptocurrency transactions?

Another question is whether it would make sense to extend the scope of the Funds Transfer Regulation and/or the Cash Control Regulation as to include cryptocurrency transactions.

The answer relating to the Cash Control Regulation can be short: it doesn't. Cryptocurrencies are normally not moved physically, making the Cash Control Regulation not such a good instrument to target cryptocurrency movements.

The answer relating to the Funds Transfer Regulation is more nuanced. This regulation basically aims at making sure that all relevant information accompanying fund transfers is there, allowing an adequate money laundering and terrorist financing check. It seems conceivable to develop and roll-out a similar system for cryptocurrency transactions. The entities that would have to fulfil the requirements could be the intermediaries through which the transactions run. Going forward, this could be a valuable add-on to the existing framework.

5.6. Is there a need for a more comprehensive approach, introducing license requirements for cryptocurrencies?

A difficult question is whether a more intrusive approach towards regulating the crypto market is warranted. As we have seen throughout this research, the EBA is a strong advocate of developing a tailored and more comprehensive framework for cryptocurrencies in time, including license requirements for cryptocurrency service providers. Part of such framework would be to create a virtual currency scheme governance authority that is accountable to the regulator.[416] An interesting line of thought for future regulation could indeed be to create or impose a "middleman", where the use of blockchain or other distributed ledger technology has cut out such middleman, as this will allow the regulator to attach regulation to an identifiable person, thus contributing to enhanced compliance and effective enforcement.

[416] See 4.2.4 The coming of age of the inclusion of cryptocurrencies into AMLD5.

Examples of tailored regimes for inspirational purposes can also be found abroad, e.g. the New York State Virtual Currency Business Activity license[417] or the proposed Maltese Virtual Currency Act and Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers[418].

The IMF also invited regulators to consider a more comprehensive approach.[419]

A similar call can be found in very recent PhD research.[420] Along the same lines, some legal doctrine suggested to revise the e-money framework and include cryptocurrencies into that revised framework.[421] Other legal doctrine, however, is more reluctant and advocates that a hard-touch regulatory approach can hinder the potential welfare-enhancing innovations coming from the ecosystem of cryptocurrencies[422]. In line herewith, it was raised that the benefits of regulation should be weighed with the costs associated therewith, and the potential deterrent effect on emerging businesses.[423]

A more comprehensive approach would include in any event the anti-money laundering and counter terrorist financing framework, because it would refer to AMLD5. Because of that, for the purposes of this research, the question is very interesting, but out of scope. Therefore, we will not elaborate it further.

5.7. Is it not best to introduce an outright ban for some aspects linked to some cryptocurrencies?

The question arises whether some aspects relating to some cryptocurrencies should not just be banned and criminally sanctioned. To mind come the mixing process attached to Dash's feature PrivateSend and Monero's RingCT, stealth addresses and Kovri-project. In essence, these features are designed to make cryptocurrency users untraceable. But why is such degree of anonymity truly necessary? Would allowing this not veer too far towards criminals? Imposing a ban for such aspects surrounding cryptocurrencies that are aimed at making it impossible to verify their users and criminally sanctioning these aspects seems to be in line with the Council's conclusions of April 2018

---

417 The regulatory framework can be accessed via: https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf. A concise analysis can be found in P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 64-65.

418 Malta positions itself as a leader in distributed ledger technology regulation. In February 2018 the Parliamentary Secretary for Financial Services, Digital Economy and Innovation within the Office of the Prime Minister, issued a consultation document on the establishment of a Malta Digital Innovation Authority, a Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers, and a Virtual Currency Act. The consultation was recently closed on 9 March 2018, but the results have yet to be made public. It will be interesting to follow-up on this and assess the future framework for potential inspiration of future EU legislation. See: Consultation Document on "The establishment of the Malta Digital Innovation Authority; the Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers; and a Virtual Currency Act", February 2018, https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF; also see S. OZELLI, "Malta Emerges as World's Cryptocurrency Hub Despite EU's TAX3 Investigation: Expert Take", June 2018, https://cointelegraph.com/news/malta-emerges-as-world-s-cryptocurrency-hub-despite-eu-s-tax3-investigation-expert-take.

419 IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 36.

420 N. VANDEZANDE, *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 310.

421 P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 59.

422 See H. NABILOU and A. PRÜM, "Ignorance, debt and cryptocurrencies: the old and the new in the law and economics of concurrent currencies", May 2018, 40p. (electronically available via https://ssrn.com/abstract=3121918).

423 T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, http://digitalcommons.law.msu.edu/jbsl, 213.

on how to respond to malicious cyber activities, under which that the use of ICT for malicious purposes is unacceptable.[424]

Whatever the answer may be, we must again avoid being naive: even if a ban would be imposed, how do we detect a breach, given that the purpose of the object of the ban just is to obscure identities?[425] Nevertheless, it would be worthwhile to consider introducing a ban. If authorities then bump into the prohibited activities, they have a legal basis for prosecution, insofar not yet available. Possibly, imposing a ban could also have a deterrent effect. Of course, again there is the tension with data protection, but arguably in the balance of things the interest of authorities and society to more effectively combat money laundering, terrorist financing and tax evasion via well-defined specific bans outweighs the interest of persons desiring to hide their identities completely.

In any event, imposing a ban should always be focused on specific aspects facilitating the illicit use of cryptocurrency too much. We are not in favour of general bans on cryptocurrencies or barring the interaction between cryptocurrency business and the formal financial sector as a whole, such as is the case in China for example.[426] That would go too far in our opinion. As long as good safeguards are in place protecting the formal financial sector and more in general society as a whole, such as rules combating money laundering, terrorist financing, tax evasion and maybe a more comprehensive set of rules aiming at protecting legitimate users (such as ordinary consumers and investors), that should be sufficient.

5.8. Is the European level the appropriate one to tackle money laundering, terrorist financing and tax evasion via cryptocurrency transactions?

Cryptocurrency transactions and crypto players are not bound by borders. Therefore, it is certain that the national level is not the right level to address money laundering, terrorist financing and tax evasion via cryptocurrencies. The European level is more appropriate. Even more appropriate, however, is the international level, as crypto activity is also not limited by the European border. Therefore, international collaboration, e.g. in the context of the UN Office on Drugs and Crime, the FATF and the Egmont Group, is crucial to successfully impose and enforce rules on combating money laundering, terrorist financing and tax evasion.[427]

From a regulatory perspective, a G20 initiative on a global framework for regulating and overseeing cryptocurrencies, to the extent necessary, would be welcome.[428] As it stands now, a first step toward a unified regulation of cryptocurrencies is expected to be taken at this level[429] in July 2018.[430] It will be

---

[424] See: http://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/.

[425] With respect to Dash's PrivateSend, a line of thought here could be to assess to what extent the masternodes could be targeted. If that would be possible, sanctioning would arguably be easier: if you shut the masternodes down who facilitate the mixing process, the process in itself may not be available any longer.

[426] See e.g. IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 28 and 35.

[427] And probably, more work needs to be done here: see IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 36; also see P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 74 and 76.

[428] T. MANDJEE, "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, http://digitalcommons.law.msu.edu/jbsl, 216; S. TEAGUE, "G20 ministers wrestle with cryptocurrency oversight", 29 March 2018, https://www.euromoney.com/article/b17jt5vnb3fn3m/g20-ministers-wrestle-with-cryptocurrency-oversight?utm_source=FX%20this%20week%20v2&utm_medium=email%20editorial&utm_content=Editorial&utm_campaign=636579242347129780&utm_term=G20%20ministers%20wrestle%20with%20cryptocurrency%20oversight.

[429] In a communiqué issued in preparation of the last G20 meeting in March 2018, the Financial Stability Board ("***FSB***") pointed out that its initial assessment is that crypto-assets do not pose risks to global financial stability at this time, though this could change in the future. At the same time the FSB stressed that crypto-assets raise a host of issues around consumer and investor protection, as well as their use

interesting to see which regulatory proposals make it to the regulatory drawing board. In any event, it would be good to see the EU take a leading role in this context and, to the extent feasible, lead by example through already adopting EU standards for cryptocurrencies.

to shield illicit activity and for money laundering and terrorist financing, which need to be addressed. See: FSB, "Communiqué to G20 Finance Ministers and Central Bank Governors", 13 March 2018, http://www.fsb.org/wp-content/uploads/P180318.pdf.

430 The G20 asked the FSB, in consultation with other international standard-setting bodies, including CPMI and IOSCO, and FATF to report in July 2018 on their work on crypto-assets (see: G20, Communiqué, 19-20 March 2018, https://g20.org/sites/default/files/media/communique_-_fmcbg_march_2018.pdf). See also: N. DE, "G20 Calls for Crypto Regulation Recommendations By July", March 2018, https://www.coindesk.com/g20-calls-crypto-regulation-recommendations-july/; D. POLLOCK, "G20 and Cryptocurrencies: Baby Steps Towards Regulatory Recommendations", March 2018, https://cointelegraph.com/news/g20-and-cryptocurrencies-baby-steps-towards-regulatory-recommendations; C. GEORGACOPOULOS, "Banks And Cryptocurrencies Global Evaluation: Europe", April 2018, https://cointelegraph.com/news/banks-and-cryptocurrencies-global-evaluation-europe.

6. WHAT ABOUT BLOCKCHAIN?

The reader will have noticed that our overview and assessment of the regulatory framework almost entirely relates to cryptocurrencies. This has been done deliberately so.

As aforementioned and evidenced throughout this research, blockchain is technology on which a cryptocurrency can run. The scope of blockchain is, however, much wider than that of cryptocurrencies. It can be applied in a large variety of sectors (e.g. trade and commerce, healthcare, governance, …), has numerous potential promising applications, e.g. relating to pledging of collateral, the registration of shares, bonds and other assets[431], the operation of land registers, etc.

Therefore, it would be too blunt to associate blockchain with money laundering, terrorist financing or tax evasion. It is just technology, which is not designed to launder money, facilitate terrorist financing or evade taxes, and has numerous applications throughout the whole lawful economy. It would not be wise to discourage future innovations in this respect by submitting blockchain and fintechs exploring its use cases to burdensome requirements, simply because of one of the applications using blockchain technology, cryptocurrencies, is used illicitly by some[432]. Admittedly, cryptocurrencies are the first well known application putting blockchain technology into the spotlight, but nowadays blockchain has clearly outgrown the context of cryptocurrencies.

Therefore, we suggest to leave blockchain be from a money laundering, terrorist financing and tax evasion perspective and focus on the illicit use cases of cryptocurrencies.

[431] CPMI, "Digital currencies", November 2015, https://www.bis.org/cpmi/publ/d137.pdf, 15.

[432] Also see P. VALCKE, N. VANDEZANDE and N. VAN DE VELDE, "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 76 and 77; G. LILIENTHAL and N. AHMAD, "Bitcoin: is it really coinage?", 2018, Computer and Telecommunications Law Review, 24(3), 49-56.

REFERENCES

- ABIOLA, L. K., 'Ethereum (ETH) Co-Founder Provides Answer To Long-Lived Supply Limit Question', April 2018, https://oracletimes.com/ethereum-eth-co-founder-provides-answer-to-long-lived-supply-limit-question/.
- ADAMS, C., "Stellar Lumens Vs Ripple", March 2018, https://www.investinblockchain.com/stellar-lumens-vs-ripple/.
- ANTONOVICI, A., "Cardano's Emurgo and SK's Metaps Plus Partner to Accept ADA", May 2018, https://cryptovest.com/news/cardanos-emurgo-and-sks-metaps-plus-partner-to-accept-ada/.
- ASOLO, B., "What are Atomic Swaps?", May 2018, https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/.
- BANQUE DE FRANCE, "Les dangers liés au développement des monnaies virtuelles: l'exemple de bitcoin", in Focus, no. 10, 5 December 2013, https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus-10-stabilite-financiere.pdf, 6p.
- BANTEKAS, I. and S. NASH, S., *International Criminal Law*, Routledge-Cavendish, 2007, 640p.
- BLUMBERG, J., "We Need To Shut Bitcoin And All Other Cryptocurrencies Down. Here's Why.", March 2018, https://www.forbes.com/sites/jasonbloomberg/2018/03/10/we-need-to-shut-bitcoin-and-all-other-cryptocurrencies-down-heres-why/#1dbed32b1bca.
- BOLLEN, R., "The Legal Status of Online Currencies: Are Bitcoins the Future?", Journal of Banking and Finance Law and Practice 2013, 38p. (electronically available via http://ssrn.com:80/abstract=2285247).
- BOVAIRD, C., "What to know before trading Monero", May 2017, https://www.coindesk.com/what-to-know-before-trading-monero/.
- BOVAIRD, C., "Why the crypto market has appreciated more than 1,200% this year", November 2017, https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#3906c8d6eed3.
- BRATSPIES, R.M., "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 49p. (electronically available via https://ssrn.com/abstract=3141605).
- BRITO, J., SHADAB, H., and CASTILLO, A., "Bitcoin financial regulation: securities, derivatives, prediction markets & gambling", 24 July 2014, 78p. (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423461).
- BRYANS, D., "Bitcoin and Money Laundering: Mining for and Effective Solution" Indiana Law Journal, 2014, Vol. 89: Iss. 1, Article 13, 32p. (electronically available via https://www.repository.law.indiana.edu/ilj/vol89/iss1/13).
- BUCHKO, S., "How Long do Bitcoin Transactions Take?", December 2017, https://coincentral.com/how-long-do-bitcoin-transfers-take/.
- BUCK, J., "First BTC-LTC Lightning Network Swap Completed, Huge Potential", November 2017, https://cointelegraph.com/news/first-btc-ltc-lightning-network-swap-completed-huge-potential.
- CHOHAN, U.W., "International Law Enforcement Responses to Cryptocurrency Accountability: Interpol Working Group", Discussion Paper, 3 April 2018, 8p.

- CITY OF ZION, "Coopetition: A New Approach to Decentralization", December 2017, https://medium.com/proof-of-working/decentralization-from-coopetition-b10d7ce3b9d.
- COM/2016/0450, "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", 6 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0450&qid=1523358551244&from=EN.
- COMMISSION STAFF WORKING DOCUMENT Accompanying the document "Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations", COM(2017) 340 final, Annex, Part 2, https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF, 85.
- COMMISSION STAFF WORKING DOCUMENT 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/2016/0223 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN.
- Consultation Document on "The establishment of the Malta Digital Innovation Authority; the Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers; and a Virtual Currency Act", February 2018, https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF.
- Council conclusions on the fight against the financing of terrorism, 12 February 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/02/12/conclusions-terrorism-financing/.
- Council Directive (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market, *OJ L* 193, 19 July 2016 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1164&from=EN).
- Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, *OJ L* 342, 16 December 2016, 1 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2258&from=EN).
- Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, as amended from to time, as regards mandatory automatic exchange of information in the field of taxation; this Directive was very recently, on 25 May 2018, amended again with rules relating to the mandatory automatic exchange of information in the field of taxation for reportable cross-border arrangements and reporting duties of intermediaries (see a first analysis: https://www.tiberghien.com/en/1282/new-reporting-obligation-for-cross-border-arrangements-council-directive-approved-25-may-2018).
- Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, *OJ L* 166, 28 June 1991, 77 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31991L0308&from=EN).

- CPMI, "Digital currencies", November 2015, https://www.bis.org/cpmi/publ/d137.pdf, 21p.
- CPMI, "Distributed ledger technology in payment, clearing and settlement – An analytical framework", February 2017, https://www.bis.org/cpmi/publ/d157.pdf, 23p.
- DANNEN, C., *Introducing Ethereum and Solidity – Foundations of Cryptocurrency and Blockchain Programming for Beginners*, Apress, 2017, 185p.
- DE, N., "G20 Calls for Crypto Regulation Recommendations By July", March 2018, https://www.coindesk.com/g20-calls-crypto-regulation-recommendations-july/.
- Delaware General Assembly, Senate Bill 69, https://legis.delaware.gov/BillDetail?legislationId=25730;
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *OJ L* 141, 5 juni 2015, 73 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=En).
- Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, *OJ L* 344, 28 December 2001, 76, (electronically available via https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF).
- Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *OJ L* 309, 25 November 2005, 15 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN).
- DUPONT, B., "The cyber security environment to 2022 Trends, drivers and implications", a study prepared for The National Cyber Security Directorate, Public Safety Canada, 2012, 44p. (electronically available via http://ssrn.com/abstract=2208548).
- EBA, "EBA Opinion on 'virtual currencies'", 4 July 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf, 46p.
- ECB, "Virtual Currency Schemes", October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, 53p.
- ECB, "Virtual Currency Schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 37p.
- Enria, A., Chairperson of EBA, "Designing a Regulatory and Supervisory Roadmap for FinTech", 9 March 2018, http://www.eba.europa.eu/documents/10180/2151635/Andrea+Enria%27s+speech+on+FinTech+at+Copenhagen+Business+School+090318.pdf, 11p.
- EP Report 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, 9

March 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN#title1.

- ESMA, EBA & EIOPA, "Warning on the risks of Virtual Currencies https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf, 3p.
- ETTO, F., "Know Your Coins: Public vs. Private Cryptocurrencies", September 2017, https://www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588.
- European Parliament legislative resolution of 19 April 2018 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)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0178+0+DOC+PDF+V0//EN.
- EY, "IFRS – Accounting for crypto-assets", March 2018, http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf, 21p.
- EY, "Research: initial coin offerings (ICOs)", December 2017, http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf, 43p.
- FATF, "International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations", February 2012, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf, 132p.
- FATF, "Report on emerging terrorist financing risks", October 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf, 47p.
- FATF, "The Forty Recommendations", 20 June 2003, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf, 7p.
- FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 15p.
- Faulkner, J., *Getting started with Cryptography in .NET*, München BookRix, 2016, 121p.
- FINCK, M., "Blockchains and Data Protection in the European Union", Max Planck Institute for Innovation & Competition Research Paper No. 18-01, 30 November 2017, 32p. (electronically available via https://ssrn.com/abstract=3080322).
- FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", February 2018, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en, 11p.
- FLEDER, M., KESTER, M.S., and PILAI, S., "Bitcoin Transaction Graph Analysis", January 2014, 8p. (electronically available via http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf).

- FLOYD, D., "$6.3 Billion: 2018 ICO Funding Has Passed 2017's Total", April 2018, https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/).
- FSB, "Communiqué to G20 Finance Ministers and Central Bank Governors", 13 March 2018, http://www.fsb.org/wp-content/uploads/P180318.pdf.
- G20, Communiqué, 19-20 March 2018, https://g20.org/sites/default/files/media/communique_-_fmcbg_march_2018.pdf.
- GEORGACOPOULOS, C., "Banks And Cryptocurrencies Global Evaluation: Europe", April 2018, https://cointelegraph.com/news/banks-and-cryptocurrencies-global-evaluation-europe.
- GLAZER, P., "An Overview of Privacy Coins", February 2018, https://hackernoon.com/an-overview-of-privacy-tokens-19f6af8077b7.
- GOLDBERG, S., "Mythbusting: Blockchain and Cryptocurrencies Edition", May 2018, http://paymentsjournal.com/mythbusting-blockchain-and-cryptocurrencies-edition/.
- GRINBERG, R., "Bitcoin: An Innovative Alternative Digital Currency", Hastings Science & Technology Law Journal, 2011, Vol. 4, 50p. (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857).
- GUP, B.E, "What Is Money? From Commodities to Virtual Currencies/Bitcoin" (14 March 2014), 12p. (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172).
- HACKER, P. and THOMALE, C., "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", November 2017, 45p. (electronically available via https://ssrn.com/abstract=3075820).
- HAUBEN, C., "Bitcoin en EU-recht: de virtuele vreemde eend in de bijt" in M. E. STORME and F. HELSEN (eds.), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia , 2017, 79-104.
- HELLER, D., "The implications of digital currencies for monetary policy", in-depth analysis commissioned by the Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, May 2017, 12p. (electronically available via http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/602048/IPOL_IDA(2017)602048_EN.pdf).
- HERLIN-KARNELL, E., and RYDER, N., "The robustness of EU Financial Crimes Legislation: A Critical review of the EU and UK Anti-Fraud and Money Laundering Scheme", 2017, European Business Law Review, No. 4, 1-39.
- HIGGINS, S., "How True Anonymity Made Darkcoin King of the Altcoins", May 2014, https://www.coindesk.com/true-anonymity-darkcoin-king-altcoins/.
- HILEMAN, G. and RAUCHS, M, "Global Cryptocurrency Benchmarking Study", Cambridge Centre for Alternative Finance, 2017, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, 115p.
- HOLDEN, W., "Bringing Blockchain to Land Registry", January 2018, https://www.blockchain-expo.com/2018/01/blockchain/bringing-blockchain-land-registry/.
- HOUBEN, R., "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 193-208.

- IMF Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 42p.
- JAGATI, S., "Ethereum's Proof of Stake Protocol Under Review", April 2018, https://cryptoslate.com/ethereums-proof-of-stake-protocol-in-review/.
- JAYACHANDRAN, P. "The difference between public and private blockchain", May 2017, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.
- KAPLAN, A., "Who accepts Ethereum as payment 2018 (List of companies that accept Ethereum)", May 2018, https://smartereum.com/2072/accepts-ethereum-payment-2018-list-companies-accept-ethereum-mon-may-28/.
- KAPLANOV, N.M., "Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation", Temple Law Review 2012, 46p. (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203).
- KEATINGE, T., CARLISLE, D., and KEEN, F., "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 87p. (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.
- KHATWANI, S., "NEO Cryptocurrency: Everything You Need to Know about China Ethereum", December 2017, https://coinsutra.com/neo-cryptocurrency/.
- KIAYIAS, A., RUSSEL, A., DAVID, B. and OLIYNYKOV, R., "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", August 2017, https://iohk.io/research/papers/?__hstc=64163184.47e0ede3cd3368ac41d33e513fea0c1b.1525905532910.1527544936508.1527699072699.9&__hssc=64163184.7.1527699072699&__hsfp=2761973715#9BKRHCSI.
- Laga, "Initial Coin Offerings - Legal qualification and regulatory challenges", March 2018, https://www.slideshare.net/fintechbelgium/fintech-belgium-meetup-on-icos-080318-laurent-godts, 9p.
- LEE, S., "Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That", April 2018, https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/.
- LEE, S., "Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0", January 2018, https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#68781282180b.
- LENG, S., "Beijing bans bitcoin, but when did it all go wrong for cryptocurrencies in China?", February 2018, http://www.scmp.com/news/china/economy/article/2132119/beijing-bans-bitcoin-when-did-it-all-go-wrong-cryptocurrencies.
- LERIDER, M., "Clarification on NEO, GAS and Consensus Nodes", August 2017, https://medium.com/@MalcolmLerider/clarification-on-neo-gas-and-consensus-nodes-aa94d4f4b09.

- LERIDER, M., "What is NEO Smart Economy?", August 2017, https://medium.com/@MalcolmLerider/what-is-neo-smart-economy-381a4c6ee286.
- LEVENSON, N., "NEO versus Ethereum: Why NEO might be 2018's strongest cryptocurrency", December 2017, https://hackernoon.com/neo-versus-ethereum-why-neo-might-be-2018s-strongest-cryptocurrency-79956138bea3.
- LEWIS, R., MCPARTLAND, J. and RANJAN, R., "Blockchain and financial market innovation", Economic Perspectives, Issue 7, 2017, Federal Reserve Bank of Chicago, 13p. (electronically available via https://www.chicagofed.org/publications/economic-perspectives/2017/7).
- LILIENTHAL, G. and AHMAD, N, "Bitcoin: is it really coinage?", 2018, Computer and Telecommunications Law Review, 24(3), 49-56.
- LUCKING, D., and O'HANLON, C., "Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares", 26 September 2017, http://www.allenovery.com/publications/en-gb/Pages/Delaware-Passes-Law-Permitting-Companies-to-Use-Blockchain-Technology-to-Issue-and-Track-Shares-.aspx.
- MADEIRA, A., "How to make an anonymous ether transaction using WeiMixer", May 2018, https://www.cryptocompare.com/coins/guides/how-to-make-an-anonymous-ether-transaction/.
- MANDJEE, T., "Bitcoin, its Legal Classification and its Regulatory Framework", 15 J. Bus. & Sec. L. 157, 2016, http://digitalcommons.law.msu.edu/jbsl, 62p.
- MARSHALL, A., "P2P Cryptocurrency Exchanges, Explained", April 2017, https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained.
- MARTINDALE, J., "What is Litecoin? Here's everything you need to know", January 2018, https://www.digitaltrends.com/computing/what-is-litecoin/.
- MARTINET, S., "GDPR and Blockchain: Is the New EU Data Protection Regulation a Threat or an Incentive?", May 2018, https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive.
- MAXWELL, W., and SALMON, J., "A guide to blockchain and data protection", Hogan Lovells, September 2017, 22p. https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf?_sm_au_=iVV6bs5Z45DMRVfr.
- MCGRATH GOODMAN, L., "The Face Behind Bitcoin", in Newsweek, 14 March 2014, http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html.
- MOSKOV, A., "Cryptocurrency Industry Spotlight: Who is NEO's Da Hongfei?", January 2018, https://coincentral.com/cryptocurrency-industry-spotlight-neos-da-hongfei/.
- NABILOU, H. and PRÜM, A., "Ignorance, debt and cryptocurrencies: the old and the new in the law and economics of concurrent currencies", May 2018, 40p. (electronically available via https://ssrn.com/abstract=3121918).
- NASEER, H., "NEO Launches Dev Competition with $490,000 Prize Pool, Co-organized by Microsoft", November 2017, https://cryptovest.com/news/neo-launches-dev-competition-with-490000-prize-pool-co-organized-by-microsoft/.
- NEL, L., "Privacy Coins: Beginner's Guide to Anonymous Cryptocurrencies", April 2018, https://blockonomi.com/privacy-cryptocurrency/.

- NIAN, LAM PAK, "Bitcoin in Singapore: A Light-Touch Approach to Regulation", 11 April 2014, 72p. (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427626).
- NJUI, J. P., "Amazon Partnership Speculation High For Ripple (XRP) As Markets Go Crazy", May 2018, https://ethereumworldnews.com/amazon-partnership-speculation-high-for-ripple-xrp-as-markets-go-crazy/.
- OECD, "Tax Challenges Arising from Digitalisation – Interim Report", 2018, 206, No. 501.
- Opinion of the ECB of 12 October 2016 on a 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, https://www.ecb.europa.eu/ecb/legal/pdf/con_2016_49_with_technical_working_document_.pdf.
- ORCUTT, M., "No, Ripple Isn't the Next Bitcoin", January 2018, https://www.technologyreview.com/s/609958/no-ripple-isnt-the-next-bitcoin/.
- Ordonnance n° 2017-1674 du 8 de cembre 2017 relative a l'utilisation d'un dispositif d'enregistrement e lectronique partage pour la repre sentation et la transmission de titres financiers, JORF 9 december 2017, no 0287, text no 24, www.legifrance.gouv.fr/eli/ordonnance/2017/12/8/2017-1674/jo/texte.
- Ozelli, S., "Malta Emerges as World's Cryptocurrency Hub Despite EU's TAX3 Investigation: Expert Take", June 2018, https://cointelegraph.com/news/malta-emerges-as-world-s-cryptocurrency-hub-despite-eu-s-tax3-investigation-expert-take.
- PAECH, P., "Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty", LSE Law, Society and Economy Working Paper 20/2015, 26-28.
- PERPER, R., "China is moving to eliminate all cryptocurrency trading with a ban on foreign exchanges", February 2018, https://www.businessinsider.nl/china-eliminates-all-cryptocurrency-trading-2018-2/?international=true&r=US&_sm_au_=iVV6bs5Z45DMRVfr.
- PETERSON, B., "The founder of litecoin, a cryptocurrency that has gained 650% in 7 months, told us he's worried about all the scams in the nascent market", January 2018, http://www.businessinsider.com/litecoin-founder-charlie-lee-on-bitcoin-and-the-cryptocurrency-bubble-2018-1?international=true&r=US&IR=T.
- PLASSARAS, N.A., "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", Chicago Journal of International Law, 2013, 26p. (electronically available http://ssrn.com:80/abstract=2248419).
- POLLOCK, D., "G20 and Cryptocurrencies: Baby Steps Towards Regulatory Recommendations", March 2018, https://cointelegraph.com/news/g20-and-cryptocurrencies-baby-steps-towards-regulatory-recommendations.
- POPOV, S., "The Tangle", October 2017, http://iotatoken.com/IOTA_Whitepaper.pdf.
- POSNAK, E. "On the Origin of Cardano", December 2017, https://medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c.
- Q. SHENTU, Q., and YU, J., "Research on Anonymization and De-anonymization in the Bitcoin System", October 2015, 14p. (electronically available via https://arxiv.org/pdf/1510.07782.pdf).

- Ramesh, A., "Features of various Blockchains: A Comparison", February 2018, https://www.xoken.org/blog/features-of-various-blockchains-a-comparison/.
- Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, *OJ L* 309, 25 November 2005, 9 (electronically available via: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R1889&from=EN).
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, *OJ L* 141, 5 juni 2015, 1 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847).
- RIZZO, P., "Ether, Litecoin and More: Overstock Now Accepts Cryptocurrencies as Payment", August 2017, https://www.coindesk.com/ether-litecoin-overstock-now-accepts-cryptocurrencies-payment/.
- ROHR, J. and WRIGHT, A., "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets", October 2017, 115p. (electronically available via https://ssrn.com/abstract=3048104).
- ROSE O'LEARY, R., "Atomic Action: Will 2018 Be the Year of the Cross-Blockchain Swap?", January 2018, https://www.coindesk.com/atomic-action-will-2018-year-cross-blockchain-swap/.
- ROSIC, A., "What is Ethereum Casper Protocol? Crash Course", November 2017, https://blockgeeks.com/guides/ethereum-casper/.
- ROSIC, A., "What is Litecoin? A Basic Beginners Guide", December 2017, https://blockgeeks.com/guides/litecoin/.
- ROYER, S., "Bitcoins in het Belgische strafrecht en strafprocesrecht", *RW* 2016-17, No. 13, 483- 501.
- SAIDOV, U., "Cryptocurrencies: The Rise of Decentralized Money", April 2018, https://blogs.cfainstitute.org/investor/2018/04/03/cryptocurrencies-the-rise-of-decentralized-money/.
- SAMEEH, T., "What If Ripple's Transactions Can Be Fully Anonymous?", May 2017, http://www.livebitcoinnews.com/ripples-transactions-can-fully-anonymous/.
- SERRES, T., "2017's Ransomware Attacks: Could Blockchain Technology Have Prevented Them?", May 2017, https://medium.com/animal-media/2017s-ransomware-attacks-could-blockchain-technology-have-prevented-them-ed9ca6bf348b.
- SETH, S., "Is Bitcoin Banned in China?", February 2018, https://www.investopedia.com/news/bitcoin-banned-china/.
- SHAH, K, 'Ethereum Supply Limit to 120 million – Prank or Reality?', April 2018, https://www.cryptoground.com/a/ethereum-supply-limit-to-120-million.
- SHAWDAGOR, J., "Blockchain Against Tax Fraud As Tencent Partners Up With Shenzhen National Taxation Bureau", May 2018, https://bitrazzi.com/blockchain-against-tax-fraud-as-tencent-partners-up-with-shenzhen-national-taxation-bureau/.
- SHOBHIT, S., "Public, Private, Permissioned Blockchains Compared", April 2018, https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/.

- SNYERS, A. and PAUWELS, K., "ICOs in Belgium: down the rabbit hole into legal no man's land? (Part 1)", ICCLR, 2018, to be published.
- SOETEMAN, K., "Werking dBft via Neo in kaart gebracht", February 2018, https://www.computable.nl/artikel/achtergrond/technologie/6306817/5182002/werking-dbft-via-neo-in-kaart-gebracht.html.
- SPAVEN, E., "Online payment network Ripple Labs receives $3.5 Million in new funding", September 2014, https://www.coindesk.com/online-payment-network-ripple-labs-receives-3-5m-new-funding/.
- SUBERG, W., "Ban Complete: China Blocks Foreign Crypto Exchanges To Counter 'Financial Risks'", February 2018, https://cointelegraph.com/news/ban-complete-china-blocks-foreign-crypto-exchanges-to-counter-financial-risks.
- SUBERG, W., "NEO DevCon Sees Microsoft Judge Network's Potential Uses", November 2017, https://cointelegraph.com/news/neo-devcon-sees-microsoft-judge-networks-potential-uses.
- SUNDARARAJAN, S., "Chinese City to Use Blockchain In Fight Against Tax Evasion", May 2018, https://www.coindesk.com/tencent-partners-with-city-authority-to-combat-tax-evasion-with-blockchain/.
- TEAGUE, S., "G20 ministers wrestle with cryptocurrency oversight", 29 March 2018, https://www.euromoney.com/article/b17jt5vnb3fn3m/g20-ministers-wrestle-with-cryptocurrency-oversight?utm_source=FX%20this%20week%20v2&utm_medium=email%20editorial&utm_content=Editorial&utm_campaign=636579242347129780&utm_term=G20%20ministers%20wrestle%20with%20cryptocurrency%20oversight.
- TENNANT, L., "Improving the Anonymity of the IOTA Cryptocurrency", October 2017, https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20f91e77e54d88b7644658912c7d/Improving_the_Anonymity_of_the_IOTA_Cryptocurrency.pdf, 20p.
- TOWN, S., "Introduction to Stellar Lumens (XLM) – The Future of Banking", April 2018, https://cryptoslate.com/stellar-lumens/.
- TRAUTMAN, L.J., "Virtual currencies: Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?", Richmond Journal of Law and Technology, Vol. 20, No. 4, 2014, 108p. (electronically available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393537).
- TUWINER, J., "Introduction to NEO – An Open Network For Smart Economy", April 2018, https://cryptoslate.com/introduction-to-neo-an-open-network-for-smart-economy/.
- VALCKE, P., VANDEZANDE, N., and VAN DE VELDE, N., "The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4", 2015, Swift Institute Working Paper No. 2015-001, 77p.
- VALENTE, P., "Bitcoin and Virtual Currencies Are Real: Are Regulators Still Virtual?", INTERTAX, Volume 46, Issue 6 & 7, 541-549.
- VAN DE LOOVERBOSCH, M., "Crypto-effecten: tussen droom en daad", TRV-RPS 2018, 193-207.
- VAN HUMBEECK, A., "The Blockchain-GDPR Paradox", November 2017, https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047.

- VAN WIRDUM, A., "Is Bitcoin Anonymous? A Complete Beginner's Guide", November 2015, https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283/.
- VANDEZANDE, N. , *Virtual currencies: a legal framework*, Antwerp, Intersentia, 2018, 500p.
- WITZIG, P., and SALOMON, V., "Cutting out the middleman: a case study of blockchain-induced reconfigurations in the Swiss Financial Services Industry", Working Paper 1, 2018/E, the Circulation of Wealth, Université de Neuchâtel, http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf, 27p.
- World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C., http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf, 46p.
- X, "A Definitive Guide To NEO (2nd Edition)", January 2018, http://storeofvalueblog.com/posts/a-definitive-guide-to-neo/.
- X, "An introduction to IOTA", 2017, https://iotasupport.com/whatisiota.shtml.
- X, "Blockchain en GDPR: een moeilijk huwelijk", May 2018, https://www.techzine.nl/blogs/404986/blockchain-en-gdpr-een-moeilijk-huwelijk.html?redirect=1.
- X, "IOTA Coin Review", January 2018, https://hackernoon.com/iota-coin-review-6a1c73c5cfa3.
- X, "True scale of Bitcoin ransomware extortion revealed", MIT Technology Review, April 2018, https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/.
- X, "What is NEO, and what is GAS?", September 2017, https://hackernoon.com/what-is-neo-and-what-is-gas-5b9828a1aa65.
- ZAINUDDIN, A., "Coins, Tokens & Altcoins: What's the Difference?", 2017, https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/.
- ZAINUDDIN, A., "Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies", 2017, https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/.
- ZETZSCHE, D., BUCKLEY, R.P., ARNER, D.W., and FÖHR, L., "The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators", November 2017 (electronically available via https://ssrn.com/abstract=3072298), 47p.

- http://data.consilium.europa.eu/doc/document/ST-15849-2017-INIT/en/pdf.
- http://docs.neo.org/en-us/index.html.
- http://drapis.com.
- http://ethdocs.org/en/latest/introduction/history-of-ethereum.html.
- http://fortune.com/2018/03/14/playboy-cryptocurrency-vice-vit-crypto/.

- http://www.consilium.europa.eu/en/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/.
- http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml).
- http://www.fsma.be/nl-in-the-picture/Article/press/div/2014/2014-01-14_virtueel.aspx.
- http://www.monero.cc.
- http://www.weidai.com/bmoney.txt.
- https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/.
- https://acceptbitcoin.cash/.
- https://anycoindirect.eu/.
- https://bitcoin.org.
- https://bitcoin.org/bitcoin.pdf.
- https://bitcoin.org/en/faq#who-created-bitcoin.
- https://bitsane.com/exchange/xrp-eur.
- https://bittrex.com/home/markets.
- https://btcdirect.eu/.
- https://cardanodocs.com/cardano/monetary-policy/.
- https://cardanodocs.com/introduction/#cryptocurrency-basics.
- https://coinfalcon.com.
- https://coinmarketcap.com/charts/.
- https://coinmarketcap.com/coins/views/all/.
- https://cryptocoincharts.info/markets/info.
- https://cryptocurrencyfacts.com/asic-mining-basics/.
- https://cryptonote.org/whitepaper.pdf.
- https://digiconomist.net/bitcoin-energy-consumption.
- https://docs.dash.org/en/latest/introduction/features.html.
- https://docs.dash.org/en/latest/introduction/features.html#privatesend.
- https://docs.dash.org/en/latest/masternodes/understanding.html.
- https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en.
- https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/criminal-justice/financial-crime_en.
- https://ec.europa.eu/taxation_customs/sites/taxation/files/com_2016_825_en.pdf.
- https://ethereumprice.org/what-is-ethereum/.

- https://eur-lex.europa.eu/procedure/EN/2016_208.
- https://exmo.com/en/news_view?id=1912.
- https://geti2p.net/en/.
- https://getmonero.org/community/merchants/.
- https://getmonero.org/get-started/what-is-monero/.
- https://getmonero.org/resources/about/.
- https://getmonero.org/resources/moneropedia/cryptocurrency.html.
- https://getmonero.org/resources/moneropedia/fungibility.html.
- https://github.com/dashpay/dash/wiki/Whitepaper.
- https://hitbtc.com.
- https://jaxx.io.
- https://litecoin.com.
- https://litecoin.com/services#merchants.
- https://localbitcoins.com.
- https://neo.org.
- https://people.csail.mit.edu/rivest/pubs/RST01.pdf.
- https://people.xiph.org/~greg/confidential_values.txt.
- https://ripple.com.
- https://ripple.com/build/xrp-ledger-consensus-process/.
- https://ripple.com/insights/ripple-escrows-55-billion-xrp-for-supply-predictability/.
- https://ripple.com/insights/ripple-receives-new-yorks-first-bitlicense-institutional-use-case-digital-assets/.
- https://ripple.com/use-cases/banks/.
- https://ripple.com/xrp/.
- https://ripple.com/xrp/market-performance/.
- https://stellar.shop/products.
- https://support.coinbase.com/customer/en/portal/topics/601112-wallet-services/articles.
- https://support.coinbase.com/customer/portal/articles/2911542.
- https://support.microsoft.com/nl-be/help/13942/microsoft-account-add-money-with-bitcoin.
- https://vapourdepot.com/.
- https://whycardano.com.
- https://www.binance.com.
- https://www.bitcoincash.org.

- https://www.bitcoincash.org/en/.
- https://www.bitfinex.com.
- https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=235707311.
- https://www.cardano.org.
- https://www.cardano.org/en/ada-distribution-audit/.
- https://www.cardano.org/en/philosophy/.
- https://www.cardano.org/en/the-daedalus-wallet/.
- https://www.cardano.org/en/what-is-cardano/.
- https://www.coinbase.com.
- https://www.coindesk.com/lot-polish-airlines-accept-bitcoin/.
- https://www.coinwarz.com/cryptocurrency.
- https://www.cryptomercado.com.
- https://www.dash.org.
- https://www.dash.org/merchants/.
- https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.
- https://www.ethereum.org.
- https://www.ethereum.org/ether.
- https://www.ethereum.org/foundation.
- https://www.expedia.com/Checkout/BitcoinTermsAndConditions.
- https://www.hotelginebra.com.es/welcome/ada/.
- https://www.investopedia.com/terms/m/mediumofexchange.asp.
- https://www.investopedia.com/terms/p/premining.asp.
- https://www.iota.org.
- https://www.iota.org/get-started/faqs.
- https://www.kraken.com.
- https://www.ledgerwallet.com/products.
- https://www.litebit.eu/.
- https://www.luno.com.
- https://www.openbazaar.org.
- https://www.preludebreakfast.com.
- https://www.reddit.com/r/NEO/comments/6su31n/here_are_some_things_you_should_know_if_you_are/.
- https://www.sproutgrowers.world/product/sprout-grower/.

- https://www.stellar.org.
- https://www.stellar.org/about/.
- https://www.stellar.org/about/mandate/.
- https://www.stellar.org/developers/guides/walkthroughs/stellar-smart-contracts.html.
- https://www.stellar.org/how-it-works/stellar-basics/.
- https://www.stellar.org/lumens/.
- https://www.tapjets.com.
- https://www.virgin.com/richard-branson/bitcoins-space.
- https://www.xrpchat.com/topic/5679-ripple-xrp-merchants-directory/.

More and more regulators are worrying about criminals who are increasingly using cryptocurrencies for illegitimate activities like money laundering, terrorist financing and tax evasion. The problem is significant: even though the full scale of misuse of virtual currencies is unknown, its market value has been reported to exceed EUR 7 billion worldwide. This paper prepared by Policy Department A elaborates on this phenomenon from a legal perspective, focusing on the use of cryptocurrencies for financial crime, money laundering and tax evasion. It contains policy recommendations for future EU standards.

PE 619.024
IP/A/TAX3/2018-03

Print ISBN 978-92-846-3199-5 | doi:10.2861/280969 | QA-03-18-060-EN-C
PDF ISBN 978-92-846-3200-8 | doi:10.2861/263175 | QA-03-18-060-EN-N