STUDY

Requested by the ECON committee

European Parliament

Crypto-assets

Key developments, regulatory concerns and responses

Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies
Authors: Prof. Dr. Robby HOUBEN & Alexander SNYERS
PE 648.779 - April 2020

EN

Crypto-assets

Key developments, regulatory concerns and responses

Abstract

This study, prepared by Policy Department A, sets out recent developments regarding crypto-assets. These relate mainly to the continuing use of crypto-assets for money laundering and terrorist financing, the massive growth of private "tokens" used to raise funds, and to the emergence of stablecoins and central bank digital currencies. The study, furthermore, addresses key regulatory concerns, taking into account these recent developments, and suggests regulatory responses.

This document was requested by the European Parliament's Committee on Economic and Monetary Affairs.

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
L-2929 - Luxembourg
Email: Poldep-Economy-Science@ep.europa.eu

Manuscript completed: April 2020
Date of publication: April 2020

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

DISCLAIMER AND COPYRIGHT

For citation purposes, the study should be referenced as: Prof. Dr. Houben, R., Snyers, A., *Crypto-assets – Key developments, regulatory concerns and responses*, Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.

CONTENTS

LIST OF ABBREVIATIONS

ADA	Cardano
AML	Anti-money laundering
AMLD4	Fourth Anti-Money Laundering Directive (Directive (EU) 2015/849)
AMLD5	Fifth Anti-Money Laundering Directive (Directive (EU) 2018/843)
BIS	Bank for International Settlements
BTC	Bitcoin
CBDC	Central bank digital currency
CPMI	Committee on Payments and Market Infrastructures
CFT	Countering the financing of terrorism
CRD	Capital Requirements Directive (Directive 2013/36/EU)
CRPT	Crypterium
CRR	Capital Requirements Regulation (Regulation (EU) 575/2013)
DAI	Multi-Collateral DAI
DASH	Dash
DLT	Distributed Ledger Technology
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
EMD2	Second Electronic Money Directive (Directive 2009/110/EC)
ESAs	European Supervisory Authorities (the EBA, EIOPA and ESMA)
ESMA	European Securities and Markets Authority
ETH	Ether
FATF	Financial Action Task Force

FIL	Filecoin
FIU	Financial intelligence unit
FSB	Financial Stability Board
GNT	Golem
GUSD	Gemini Dollar
ICO	Initial Coin Offering
IMF	International Monetary Fund
INR	Interpretative Note to Recommendation
IOSCO	International Organization of Securities Commissions
IPO	Initial Public Offering
ITO	Initial Token Offering
JPM	J.P. Morgan Coin
MAR	Market Abuse Regulation (Regulation (EU) No 596/2014)
MiFID	Markets in Financial Instruments Directive
ML/TF	Money laundering/terrorist financing
NCA	National Competent Authority
PAX	Paxos Standard
PoS	Proof-of-Stake
PoW	Proof-of-Work
PSD2	Second Payment Services Directive (Directive 2015/2366/EU)
TIPS	TARGET Instant Payments Settlement
USDT	Tether
XMR	Monero

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

At the start of 2020, over 5,100 crypto-assets exist with a total market capitalisation exceeding $250 billion.

Both lawful and unlawful crypto-markets exist. Most legal activity in crypto-assets – and in particular in cryptocurrencies – takes place on crypto-exchanges. It relates mostly to the use of cryptocurrencies for speculative purposes. The illegal activity includes, amongst others, the buying and selling of illegal goods or services online in darknet marketplaces, money laundering, evasion of capital controls, payments in ransomware attacks and thefts. In this context, cryptocurrencies function mostly as a payment instrument. Remarkable is that almost half of all (yearly) transactions in Bitcoin can be linked to illegal activity according to Australian researchers who employed specific algorithms to analyse transaction data. As the crypto-market is still dominated by Bitcoin, with a dominance in terms of total market capitalisation exceeding 63% ($159 billion), this is an important observation.

As such, the use of cryptocurrencies for criminal purposes is not new and was already covered by our 2018 study *Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion*. Since then, there are, however, interesting developments as regards blind spots in the fight against financial crime and how to address the illegal use of crypto-assets via regulation. This study addresses these new developments.

In addition, and outside of the context of the use of crypto-assets in an illegal context, two notable developments since our previous study are (i) the massive growth of the number of so-called private "tokens" issued on existing platforms in order to raise funds; and (ii) the emergence of so-called "stablecoins" and central bank digital currencies (CBDCs). These trends have caused various regulatory authorities, standard-setting bodies and legal scholars to shift their focus and expand their vocabulary from the term "cryptocurrencies" to the broader term of "crypto-assets". This study focusses on crypto-assets in this broader sense, and hence, also scrutinizes tokens, stablecoins and CBDCs.

As regards CBDCs an observation is that these are not yet a reality, leaving some pilot programmes aside. Therefore, as it stands, it is too early to tell whether CBDCs will indeed be(come) game changers for payments. More research needs to be done. An interesting line of thought in this context, that links CBDCs with compliance with laws, is that replacing anonymous, untraceable cash with a public, traceable CBDC, could theoretically mark the end of many money laundering and criminal activities, although from a political perspective such scenario is probably unlikely.

Regarding stablecoins, various examples are already in circulation. Most stablecoins have a local footprint. Recently, however, new stablecoin initiatives have emerged. The most important one is probably Facebook's Libra project. These new initiatives are built on top of existing, large and/or cross-border user bases. They have the potential to scale very quickly to achieve a global or other substantial footprint and are commonly referred to as "global stablecoins". Global stablecoins could provide various benefits to the financial system, most notably by lowering transaction fees in retail cross-border payments and facilitating financial inclusion, yet their global scale also poses new challenges and risks to, amongst others, financial stability and monetary policy.

Global stablecoins are not the only regulatory concern the legislator faces today. Another concern is that, at present, EU financial laws do not prohibit financial institutions from holding or gaining exposure to crypto-assets or from offering services relating to crypto-assets. This can prove problematic: most crypto-assets exhibit a high degree of volatility or have not yet proven to be truly resilient in times of financial stress. In other words, if financial institutions decide to acquire them and take them on their balance sheets or engage in activities that involve them, they could face enormous

losses. As part of a conservative prudential treatment, for now, the best way forward to deal with the uncertainty surrounding crypto-assets, is probably to deduct them from a financial institution's own funds.

A continuing concern is, moreover, the use of crypto-assets for financial crime. Crypto-assets pose serious money laundering and terrorist financing risks that criminals, money launderers, terrorists and other illicit actors could exploit. The fact that they are fully digital, easily transferable, pseudonymous – and with the use of specific anonymity-enhancing technology even completely anonymous – assets that operate on a decentralised basis, makes them particularly suitable for money laundering and other criminal activities.

To address the ML/TF risks presented by cryptocurrencies - or, as the EU up until now referred to them, "virtual currencies" - the EU legislator included so-called "*custodian wallet providers*" and "*providers engaged in exchange services between virtual currencies and fiat currencies*" within the scope of the AML/CFT framework by defining them as obliged entities in AMLD5.

However, since the adoption of AMLD5 on 30 May 2018, the crypto-space has not stood still. New crypto-assets were created, new types of crypto-related services emerged and new service providers entered the crypto-market. In response to these new developments, the Financial Action Task Force (FATF) adopted changes to its Recommendations in October 2018, to clarify that they apply to financial activities involving virtual assets, as well as related service providers. In June 2019, the FATF adopted an Interpretative Note to Recommendation 15 (INR 15) to further clarify how the FATF requirements should be applied in relation to virtual assets and virtual asset service providers. The FATF also adopted new Guidance on the application of the risk-based approach to virtual assets and virtual asset service providers in June 2019. A side-by-side comparison of the latest FATF standards on virtual assets with the AML/CFT-regime for virtual currencies set-out in AMLD5 shows that the existing European AML/CFT-regime for virtual currencies already lags behind of what is considered the current international AML/CFT-standard for crypto-assets.

To bring the European AML/CFT framework up to speed with the current reality in the crypto-space, the EU could consider a number of regulatory actions. A first regulatory action to consider is to broaden the scope of the definition of virtual currencies, for instance to include tokens. Secondly, the list of obliged entities could be broadened. The following blind spots could be addressed: crypto-exchanges exchanging crypto into crypto; financial service providers who are active in the participation in and provision of financial services related to an issuer's offer and/or sale of a crypto-asset; and, trading platforms, at least insofar they are centrally operated. An interesting question is whether it would not also make sense to include issuers or offerors of crypto-assets into the list of obliged entities. Non-custodian wallet providers only provide the technical tools for others to work with and typically do not function as an intermediary so it does not make much sense to target them for AML/CFT purposes. The same holds true for coin inventors. A different approach is warranted for miners. Nowadays, coins have emerged that do not always require big energy-consuming server farms to mine, but that can be mined running a few hardware rigs at home. As it stands, such rigs can be set up by anyone, also by criminal actors. Regulators should be aware that by mining coins, directly or indirectly via front men, criminal actors can get access to clean cash. Newly mined coins are by definition "clean", so if someone (e.g., a bank) is willing to convert them into fiat currency or other crypto-assets, the resulting funds are also clean. A first regulatory step could be to try to map the use of this technique and subsequently, if it effectively proves an important blind spot, to consider appropriate counter measures.

In addition, and in view of the cross-border nature of crypto-assets and their misuse, the introduction of a European AML watchdog could have various benefits, especially if it is staffed with highly trained IT personnel capable of analysing the AML/CFT risks new technologies bring. It could help promote

information-sharing, serve as a new knowledge pool, and provide a more independent approach to AML/CFT cases in comparison to national FIUs.

When enhancing the regulatory framework with respect to criminal use of crypto-assets, the EU should be mindful to also enhance the investigative toolbox: to ensure compliance with the regulatory framework, law enforcement agencies at both EU level and Member State level must be able to detect infractions and subsequently sanction them. Therefore, the EU should continue to invest in initiatives that add to the investigative toolbox of law enforcement agencies who are trying to track down ML/TF and other illicit activities such as tax evasion via crypto-assets.

A third regulatory concern relates to investments in crypto-assets. Since the explosion of initial coin offerings in 2017, various regulators have issued statements warning people that investments in crypto-assets are very risky and often fall outside the scope of EU financial services laws, leaving investors unprotected if something goes wrong. At the same time, regulators have pointed out that, depending on their specific design features, certain crypto assets can be included in the scope of EU financial services laws. In practice, however, it is not always clear if a crypto-asset effectively falls inside the scope of the existing regulatory framework. This is not only due to the often tailored nature of crypto-assets, but also to the lack of clarity in the financial regulatory framework. These circumstances are challenging for all actors involved (including financial supervisors, crypto investment firms and crypto investors), contribute to regulatory arbitrage and generally lead to legal uncertainty. To create a level playing field and ensure adequate investor protection across the EU, a common view on the legal qualification of crypto-assets as financial instruments is required. Moreover, EU financial services laws should be brought up to speed with the unique characteristics of the crypto-sector, to allow for an effective application of existing financial regulation to crypto-assets that are financial instruments. As regards crypto-assets that do not qualify as MiFID II financial instruments, nor EMD2 electronic money, and hence, escape all EU financial regulation, the EU should, at the very least, put appropriate risk disclosure requirements in place, so that investors and/or consumers can be made aware of the potential risks prior to committing funds to these crypto-assets.

A last regulatory concern considered in this study is cybersecurity. Cybersecurity has become a major issue in the field of crypto-assets. Stolen crypto-assets typically find their way to illegal markets and are used to fund further criminal activity. Along the same lines, in the context of ransomware attacks, criminals often ask victims to pay the ransom in cryptocurrencies such as Bitcoin. Cryptocurrencies allow criminals to monetise on ransomware attacks without revealing their real-life identities, making such attacks very interesting and lucrative exploits. In the current state of the EU regulatory framework, there are no specific laws that set-out minimum standards for cybersecurity to be complied with by intermediaries who offer custodial services for crypto-assets. The EU should consider introducing such standards for intermediaries operating within the EU. To decrease the number of successful ransomware attacks involving crypto-ransoms, overall cyber-security awareness can be improved. In addition, a regulatory response could be to make it harder for criminals to use the crypto-ransoms they have collected for other, future, transactions. This could be done by blacklisting the coins used to pay a crypto-ransom.

Crypto-assets are a global phenomenon: they are created by private actors in various countries all over the world, they are cross-border in their application and infrastructure, and they are easily accessible, transferable, exchangeable and tradeable from nearly anywhere in the world. As a result, they do not only present regulatory challenges within EU borders, but far beyond. To address these challenges, regulatory authorities will have to step in. In some countries legislators have already taken action or are planning to do so. These national initiatives are not necessarily aligned with each other, leading to

regulatory arbitrage. To avoid regulatory arbitrage, rulemaking on crypto-assets should ideally take place at the European level, preferably in the execution of international standards.

1. GENERAL INFORMATION

KEY FINDINGS

- Central bank digital currencies are not yet a reality, leaving some pilot programmes aside.
- Stablecoins, on the contrary, are already in circulation. Most stablecoins have a local footprint. Recently, however, global stablecoins emerged, with Facebook's Libra project as an important example. Global stablecoins could provide various benefits to the financial system, most notably by lowering transaction fees in retail cross-border payments and facilitating financial inclusion, yet their global scale also poses new challenges and risks to, amongst others, financial stability and monetary policy.
- EU financial laws do not prohibit financial institutions from holding or gaining exposure to crypto-assets or from offering services relating to crypto-assets. This can prove problematic: most crypto-assets exhibit a high degree of volatility or have not yet proven to be truly resilient in times of financial stress.
- A continuing concern is the use of crypto-assets for financial crime. The current EU AML/CFT framework, AMLD5, already lags behind the current reality in the crypto-space and is not fully equipped for the fight against money laundering and terrorist financing.
- The introduction of a European AML watchdog could have various benefits.
- When enhancing the regulatory AML/CFT framework, the EU should be mindful to also enhance the investigative toolbox.
- The current EU financial regulatory framework is not sufficiently tailored to crypto-assets creating challenges for all actors involved, contributing to regulatory arbitrage and generally leading to legal uncertainty.
- Cybersecurity has become a major issue in the field of crypto-assets. Stolen crypto-assets typically find their way to illegal markets and are used to fund further criminal activity. In the context of ransomware attacks, criminals often ask victims to pay the ransom in cryptocurrencies such as Bitcoin.
- To avoid regulatory arbitrage, rulemaking on crypto-assets should ideally take place at the European level, preferably in the execution of international standards.

1.1. Background

At the start of 2020, over 5,100 crypto-assets exist with a total market capitalisation exceeding $250 billion[1].

Both lawful and unlawful crypto-markets exist. Most legal activity in crypto-assets – and in particular in cryptocurrencies – takes place on crypto-exchanges. It relates mostly to the use of cryptocurrencies for speculative purposes. The illegal activity includes, amongst others, the buying and selling of illegal goods or services online in darknet marketplaces, money laundering, evasion of capital controls, payments in ransomware attacks and thefts. In this context, cryptocurrencies function mostly as a payment instrument. Remarkable is that almost half of all (yearly) transactions in Bitcoin can be linked to illegal activity according to Australian researchers who employed specific algorithms to analyse transaction data. As the crypto-market is still dominated by Bitcoin, with a dominance in terms of total market capitalisation exceeding 63% ($159 billion), this is an important observation.

As such, the use of cryptocurrencies for criminal purposes is not new and was already covered by our 2018 study *Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion*[2]. Since then, there are, however, interesting developments as regards blind spots in the fight against financial crime and how to address the illegal use of crypto-assets via regulation.

In addition, and outside of the context of the use of crypto-assets in an illegal context, two notable developments since our previous study are (i) the massive growth of the number of so-called private "tokens" issued on existing platforms in order to raise funds; and (ii) the emergence of so-called "stablecoins" and central bank digital currencies (CBDCs). These trends have caused various regulatory authorities, standard-setting bodies and legal scholars to shift their focus and expand their vocabulary from the term "cryptocurrencies" to the broader term of "crypto-assets".

This study focusses on crypto-assets in the aforementioned broader sense, and hence, also relates to tokens, stablecoins and CBDCs. The study intends to introduce these new developments, and situate them against the background of the first wave of crypto-assets, which were discussed more at length in our aforementioned 2018 study.

This study, furthermore, analyses the new developments as regards blind spots in the fight against financial crime and how to address illegal use of crypto-assets via regulation.

1.2. Scope of the research

The new developments in the crypto-space, as aforementioned, will first be introduced. Subsequently, an overview of current markets will be given. Thirdly, taking into account the researched new developments and current markets, the study will focus on four key regulatory concerns, namely:

- global stablecoins, that pose new challenges and risks to, amongst others, financial stability and monetary policy;
- financial institutions holding on to crypto-assets on their balance sheets or engaging in activities that involve them;

[1] Statement made on the basis of data derived from https://coinmarketcap.com on 4 March 2020.

[2] R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, p. 100. (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

- the continuing use of crypto-assets for financial crime, particularly money laundering and terrorist financing; and
- cybersecurity as regards crypto-assets.

Relating to each concern, the study suggests a regulatory approach going forward.

It is not the intention of the study to be exhaustive: the study does not aim at addressing all developments in the crypto-space, nor at identifying all concerns related to crypto-assets or at suggesting all possible responses to the identified concerns. It does, however, attempt to highlight key developments, key concerns and key responses.

The study scrutinizes crypto-assets from a legal perspective; other perspectives are not included. We focus on the EU legal context and will not elaborate on the international or national context, unless it is relevant to better understand the European context.

The study was completed on 6 April 2020.

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

- The EU should be mindful of ongoing research and experiments relating to central bank digital currencies. It should contribute to further research to assess the viability of central bank digital currencies.
- The EU should align its actions with regard to global stablecoin projects with the ongoing work of international standard-setting bodies like the FSB.
- The EU should assess an adequate approach as regards financial institutions with crypto-assets on their balance sheets and/or dealing in crypto-assets.
- To bring the European AML/CFT framework up to speed with the current reality in the crypto-space, the EU should consider a number of regulatory actions, including: broadening the definition of virtual currencies, expanding the list obliged entities to include more crypto-gatekeepers, paying sufficient attention to the role of miners, researching whether decentralised trading facilities effectively pose AML/CFT risks.
- The EU should continue to invest in initiatives that add to the investigative toolbox of law enforcement agencies who are trying to track down ML/TF and other illicit activities such as tax evasion via crypto-assets.
- The EU could assess the development of a central bank digital currency that strikes a balance between citizens' rightful demand for user integrity, and the need to comply with AML/CFT standards, building on the work done by the EUROchain research network.
- The EU should further explore the introduction of a European AML watchdog.
- To create a level playing field and ensure adequate investor protection across the EU, the EU should consider introducing a common view on the legal qualification of crypto-assets as financial instruments. Moreover, EU financial services laws should be brought up to speed with the unique characteristics of the crypto-sector, to allow for an effective application of existing financial regulation to crypto-assets that are financial instruments.
- As regards crypto-assets that do not qualify as MiFID II financial instruments, nor EMD2 electronic money, and hence, currently escape all EU financial regulation, the EU should, at the very least, put appropriate risk disclosure requirements in place, so that investors and/or consumers can be made aware of the potential risks prior to committing funds to these crypto-assets.
- The EU should consider introducing standards for cybersecurity to be complied with by intermediaries who offer custodial services within the EU.
- The EU should follow-up on the technical feasibility of coin blacklisting – which could have a much broader application than only rebutting ransomware attacks – and the potential effects it could have on the crypto-market as a whole.

2. WHAT ARE CRYPTO-ASSETS?

2.1. A wide variety of assets

Since our 2018 study *Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion*[3], the crypto-market has changed significantly. Two of the most notable developments are (i) the massive growth of the number of so-called private "tokens" issued on existing platforms in order to raise funds and (ii) the emergence of so-called "stablecoins". These trends have caused various regulatory authorities, standard-setting bodies and legal scholars to shift their focus and expand their vocabulary from the term "cryptocurrencies" to the broader term of "crypto-assets"[4].

At present, the term "crypto-assets" is used to refer to a wide variety of assets. Despite its frequent use, there is no generally-accepted definition of what constitutes a crypto-asset. Different definitions have been adopted by regulatory authorities and standard-setting bodies for the purpose of their monitoring and supervisory work, or for other purposes:

- the **ECB Crypto-Assets Task Force** has defined the term very narrowly as "*any asset recorded in digital form that is not and does not represent either a financial claim on, or a financial liability of, any natural or legal person, and which does not embody a proprietary right against an entity*"[5];
- **IOSCO** has defined the term as "*a type of private asset that depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, and can represent an asset such as a currency, commodity or security, or be a derivative on a commodity or security*"[6];
- the **FSB** has put forward a similar definition and defines the term as "*a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value*"[7]. This definition is also referred to in **BIS** documentation[8];
- in line with the FSB's definition, the **ESMA** has defined a crypto-asset as "*a type of private asset that depends primarily on cryptography and DLT or similar technology as part of their perceived or inherent value*". ESMA uses the term to refer both to so-called 'virtual currencies' and 'digital tokens' (which it defines as "*any digital representation of an interest, which may be of value, a right to receive a benefit or perform specified functions or may not have a specified purpose or use*"). According to the ESMA, crypto-asset additionally means an asset that is not issued by a central bank[9]; and

---

3 R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, p. 100. (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

4 M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 17 (electronically available via https://ssrn.com/abstract=3306125).

5 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 7 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

6 IOSCO, "Consultation Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, 1; IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 1.

7 FSB, "Crypto-assets: work underway, regulatory approaches and potential gaps", May 2019, https://www.fsb.org/wp-content/uploads/P310519.pdf, p. 10.

8 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.

9 ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, p. 42.

- the **EBA** has defined a crypto-asset in a similar way as "*an asset that: a) depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, b) is neither issued nor guaranteed by a central bank or public authority, and c) can be used as a means of exchange and/or for investment purposes and/or to access a good or service*"[10].

With the exception of the ECB Crypto-Assets Task Force's definition (which only appears to cover what could be called traditional "non-backed" cryptocurrencies[11] (such as Bitcoin and Litecoin, etc.[12])), all of the definitions set out above have a very broad scope. Two recurring components are (i) the private nature of the asset, and (ii) the use of cryptography and DLT or similar technology.

Having regard of the scope of the ECB's mandate, the limited scope of the ECB Crypto-Assets Task Force's definition of crypto-assets is perfectly understandable. However, this study wants to go beyond and scrutinize more than solely traditional "non-backed" cryptocurrencies. Therefore, it builds further on the definition of the EBA and defines a crypto-asset as **a private digital asset that:**

a) is recorded on some form of a digital distributed ledger secured with cryptography,

b) is neither issued nor guaranteed by a central bank or public authority, and

c) can be used as a means of exchange and/or for investment purposes and/or to access a good or service[13].

Before diving deeper into the world of "crypto-assets", it should be noted that, even though the use of the term "crypto-assets" is becoming more and more widespread, there are still various legal texts and policy documents that use different terms, such as virtual currencies, coins, digital currencies or digital assets to refer to some or all types of crypto-assets[14]. If and when necessary, this study will further frame these terms within a broader taxonomy of crypto-assets.

2.2. *Summa divisio*: cryptocurrencies and tokens

Crypto-assets can take on different forms and have various characteristics[15]. From a bird's eye view, a *summa divisio* can be made between cryptocurrencies on the one hand, and tokens on the other hand.

---

[10] EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 10-11.

[11] The ECB Crypto-Asset Task Force appears to have adopted the term crypto-asset to underscore that in its opinion a cryptocurrency is not a true "currency" (i.e. it does not truly fulfil the requirements of a medium of exchange, a store of value and a unit of account), and can therefore not be referred to as such, see also below.

[12] See 2.4. Cryptocurrencies can be backed ("stable") or not, below.

[13] A reference to the perceived or inherent value of the asset having to stem at least in part from the use of cryptography and DLT or similar technology (as contained in EBA's definition), has been left out of this working definition. This has been done to ensure that it includes all types of "stablecoins" (see further below), the perceived or inherent value of which does not necessarily stem from the use of cryptography and DLT, but rather from their redeemability and backing. The working definition put forward in this study is, admittedly, very broad, but in line with recent scholarly debate (see *inter alia* A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", *TBH* 2019/2, (174) 179-181; C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 75; S. BLEMUS and D. GUEGAN, "Initial Crypto-Asset Offerings (ICOs), Tokenization and Corporate Governance", January 2019, 7 (electronically available via https://ssrn.com/abstract=3350771); F. ANNUNZIATA, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, 3-7 (electronically available via https://ssrn.com/abstract=3332485); L. PERLMAN, "A Model Crypto-Asset Regulatory Framework", May 2019, 1 (electronically available via https://ssrn.com/abstract=3370679); M. NANNINGS, "Kwalificatie van crypto-assets als effect", *TFR* 2019/12, (623) 623-625) and instrumental to the scope of the research.

[14] *Cf.* BASEL COMMITTEE ON BANKING SUPERVISION, "Designing a prudential treatment for crypto-assets", December 2019, 5 (electronically available via https://www.bis.org/bcbs/publ/d490.pdf). See also CONGRESSIONAL RESEARCH SERVICE, "Digital Assets and SEC Regulation", January 2020, 1 (electronically available via https://www.hsdl.org/?view&did=833720).

[15] A. SNYERS and K. PAUWELS, "ICOs in Belgium: down the rabbit hole into legal no man's land? Part 1", *ICCLR* 2018, Vol. 29, Issue 8, (483) 485-487; F. ANNUNZIATA, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin

Cryptocurrencies (or coins), such as Bitcoin and Litecoin, are those crypto-assets that are designed or intended to perform the roles of currency, *i.e.* to function as a general-purpose medium of exchange, a store of value and a unit of account[16]. They are intended to constitute a peer-to-peer alternative to government-issued legal tender[17].

Tokens, on the other hand, are those crypto-assets that offer their holders certain economic and/or governance and/or utility/consumption rights[18]. Broadly speaking, they are digital representations of interests, or rights to (access) certain assets, products or services[19]. Tokens are typically issued on an existing platform or blockchain to raise capital for new entrepreneurial projects, or to fund start-ups or the development of new (technologically) innovative services[20].

In some legal literature and policy documentation, cryptocurrencies are also referred to as "payment tokens", "exchange tokens" or "currency tokens"[21]. This terminology is confusing and not without its issues. Where tokens typically represent an entitlement to some asset or right, cryptocurrencies – or at least traditional "non-backed" cryptocurrencies[22] – generally do not embody intrinsic rights and entitlements[23].

Cryptocurrencies were the first type of crypto-assets to emerge, with the creation of Bitcoin already dating back to late 2008 – early 2009[24]. Tokens, which are the result of a transaction carried out by an issuer, generally in connection with the collection of financial resources[25], became widely popular by the end of 2017; a trend that persists until this day. They are, what could be called, the second generation of crypto-assets.

2.3. Cryptocurrencies *vs.* central bank digital currencies: private *vs.* sovereign coins

The emergence, and growing popularity, of cryptocurrencies and their underlying technology have inspired various central banks to investigate whether it would make sense for them to issue their own

Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, 21-24 (electronically available via https://ssrn.com/abstract=3332485).

16 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 76.

17 See also the analysis set out in R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 20-23 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

18 A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", *TBH* 2019/2, (174) 179-181; T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 21-23 (electronically available via https://ssrn.com/abstract=3337514); M. NANNINGS, "Kwalificatie van crypto-assets als effect", *TFR* 2019/12, (623) 624-625.

19 ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 42; C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 76.

20 F. ANNUNZIATA, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, 4 (electronically available via https://ssrn.com/abstract=3332485).

21 See for example EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7; S. BLEMUS and D. GUEGAN, "Initial Crypto-Asset Offerings (ICOs), Tokenization and Corporate Governance", January 2019, 9 (electronically available via https://ssrn.com/abstract=3350771); T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 20 (electronically available via https://ssrn.com/abstract=3337514).

22 See 2.4. Cryptocurrencies can be backed ("stable") or not, below.

23 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 76.

24 See https://bitcoin.org/bitcoin.pdf. For a brief historical overview see also: T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 15-17 (electronically available via https://ssrn.com/abstract=3337514).

25 F. ANNUNZIATA, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, 4 (electronically available via https://ssrn.com/abstract=3332485).

"digital currencies", for wholesale purposes, or as a complement to or a substitute for physical banknotes and coins[26]. These digital currencies are commonly referred to as central bank digital currencies (CBDCs). Simply put, a CBDC is a digital asset or a digitalised instrument issued by a central bank for the purpose of payment and settlement, in either retail or wholesale transactions[27]. Since it is issued by a central bank – and, hence is a central bank liability –, it could be described as a sovereign coin.

Various central banking and monetary policy institutions have stressed that issuing a CBDC is not contingent upon the use of a specific technology such as DLT[28].

CBDCs could have diverse benefits, yet at the same time, they also raise various (monetary policy) concerns[29]. Like cryptocurrencies, which are at the very least intended to perform the roles of currency, CBDCs are digital currencies. However, that is as far as the comparison goes. Where cryptocurrencies, a subcategory of crypto-assets, are private in nature, generally make use of some form of DLT and are not issued or guaranteed by a central bank, the opposite is true for CBDCs. A clear dividing line between cryptocurrencies, or even broader crypto-assets on the one hand, and CBDCs on the other hand, should therefore be drawn.

2.4. Cryptocurrencies can be backed ("stable") or not

The first wave of cryptocurrencies, which began with Bitcoin and hundreds of subsequent Bitcoin clones[30], are *de-facto* considered by their users as "something of value". They do not represent any underlying asset, claim or liability[31], making them prone to high price volatility[32]. They are what could be called traditional "non-backed" cryptocurrencies.

The highly volatile nature of traditional "non-backed" cryptocurrencies makes it very hard for them to truly perform the roles of currency (*i.e.* function as a medium of exchange, a store of value and a unit of account) and to become more widely adopted as such[33]. In view hereof, central banks usually refrain from using the term crypto*currencies* to refer to these crypto-assets all-together[34].

---

[26] OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 35 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf); U. BINDSEIL, "Central bank digital currency - financial system implications and control", July 2019, 2 (electronically available via https://ssrn.com/abstract=3385283).

[27] OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 2 and 9 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

[28] C. BARONTINI and H. HOLDEN, "Proceeding with caution – a survey on central bank digital currency" (BIS Papers No 101), January 2019, https://www.bis.org/publ/bppdf/bispap101.pdf, 3; ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 32 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf); OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 35 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

[29] See 3.2.1.iii, below.

[30] D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 3 (electronically available via https://ssrn.com/abstract=3414401).

[31] ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 8 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

[32] D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 6 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

[33] H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 113.

[34] *Cf.* OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 9 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

A number of cryptocurrency advocates have recognised that the severe price volatility of the first wave of cryptocurrencies is indeed a major hurdle for their acceptance as a means of payment and store of value. They have tried to address the issue at hand by introducing so-called stablecoins[35]. Simply put, a stablecoin is a variant or subcategory of cryptocurrencies typically pegged or linked to the price of another asset or a pool of assets, designed to maintain a stable value[36]. Like traditional "non-backed" cryptocurrencies, stablecoins are intended to perform the roles of currency[37]. Unlike traditional "non-backed" cryptocurrencies, which are generally decentralised[38], and do not have an identifiable issuer or at least not an institution that can easily be held accountable by or towards the coin's users, stablecoins typically represent a "claim" on a specific issuer or on underlying assets or funds, or some other right or interest[39]. They are, in other words, backed by something and not just perceived to be "something of value". Examples of stablecoins that are already in circulation are Tether (USDT)[40], Multi-collateral DAI (DAI)[41] and Gemini Dollar (GUSD)[42], among several others[43].

Stablecoins share a number of properties with "tokens" and are sometimes even identified as such[44]. Like tokens, stablecoins are typically issued on an existing blockchain and embody a claim (*vis-à-vis* an identifiable issuer or on assets backing the coins). However, whereas tokens are issued with a very specific functionality or for a specific purpose (e.g., to provide their holders ownership rights and/or dividend-like rights, or to enable access to a specific product or service)[45], stablecoins generally lack such functionality. They are intended to be used as a general-purpose medium of exchange: to enable the buying and selling of a good or service provided by someone other than the issuer. Therefore, they should be distinguished from tokens, rather than be identified as such.

2.5. Tokens can be investment tokens or utility tokens or hybrid forms thereof

Just like there is currently more than one category of cryptocurrencies, there is also more than one category of tokens. Tokens can take on different forms with diverse features[46]. Since their conception, different approaches have been developed to classify and define them[47]. Generally speaking, most

---

35 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 6 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf); G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.

36 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 2 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf). See also V. BRÜL, "Libra – A Differentiated View on Facebook's Virtual Currency Project", *Intereconomics 2020/1 (ZBW – Leibniz Information Centre for Economics)*, 55.

37 However, see with a bit more nuance also below 3.2.2 b The story of stablecoins to overcome the problem of volatility.

38 See also D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 6 (electronically available via https://ssrn.com/abstract=3414401).

39 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.

40 See https://tether.to.

41 See https://makerdao.com/en/.

42 See https://gemini.com/dollar.

43 See also C. CALCATERRA, W. A. KAAL and V. RAO, "Stable cryptocurrencies – First Order Principles", *Stanford Journal of Blockchain Law & Policy (2019)*, June 2019, 4 (electronically available via https://ssrn.com/abstract=3402701).

44 For example, the popular website https://coinmarketcap.com lists stablecoins such as Tether and DAI as tokens.

45 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7.

46 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 76; F. ANNUNZIATA, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, 21 *et seq.* (electronically available via https://ssrn.com/abstract=3332485).

47 See *inter alia* J. ROHR and A. WRIGHT, "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital

regulatory authorities and legal scholars tend to distinguish so-called "investment" or "security" tokens from so-called "utility" tokens[48].

Investment tokens – sometimes also referred to as security tokens or asset tokens – are those tokens that typically provide their holders rights in the form of ownership rights and/or entitlements that are similar to dividends[49]. A well-known example of an investment token is Bankera's "BNK token", which grants its holder a right to a weekly commission to be paid out in the cryptocurrency "ether" (ETH)[50]. Investment tokens are generally issued for the purpose of capital raising (*i.e.* through an ICO[51]) and show similarities to traditional debt and equity instruments[52]. However, the term "investment token" is also used to refer to traditional securities or other assets that have undergone the process of tokenisation (*i.e.* that have been registered on a blockchain in the form of a token)[53].

Utility tokens are those tokens that grant their holders access to a specific application, product or service often provided through a newly developed (blockchain-type) infrastructure[54]. They typically only provide access to a product or service developed by the token issuer and are not accepted as a means of payment for other products or services[55]. Hence, they differ from cryptocurrencies. Some examples of utility tokens include Golem (GNT)[56] and Filecoin (FIL)[57], which each facilitate access to a specific service, *i.e.* computing power (Golem) and data storage (Filecoin). Like investment tokens, utility tokens are also issued to collect financial resources, usually to fund the further development of the issuer's application, product or service. However, unlike investment tokens, their main purpose is not to generate future cash flows for investors, but to grant access to the issuer's application, product or service[58], and at the same time create a user base. The value of utility tokens is typically derived from

---

Markets", *Cardozo Legal Studies Research Paper No. 527*, October 2017, 7-19 (electronically available via https://ssrn.com/abstract=3048104); EY, "Research: initial coin offerings (ICOs)", December 2017, 25 (electronically available via http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf); 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, 3; P. HACKER and C. THOMALE, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", November 2017, 12 (electronically available via https://ssrn.com/abstract=3075820); P. MOMTAZ, "Initial Coin Offerings" July 2018, 7 (electronically available via https://ssrn.com/abstract=3166709); D. A. 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", *University of Luxembourg Law Working Paper No. 11/2017*, July 2018, 6-10 (electronically available via https://ssrn.com/abstract=3072298); V. BURILOV, "Utility Token Offerings and Crypto Exchange Listings: how regulation can help?", November 2018, 8-16 (electronically available via https://ssrn.com/abstract=3284049); SECURITIES AND MARKETS STAKEHOLDER GROUP, "Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets", *ESMA22-106-1338*, October 2018, 4-5 (electronically available via https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf); C. FISH, "Initial coin offerings (ICOs) to finance new ventures", *Journal of Business Venturing, 34(1)*, January 2019, 6-7 (electronically available via https://ssrn.com/abstract=3147521).

48 See *inter alia* EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7; ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 19; A. SNYERS and K. PAUWELS, "ICOs in Belgium: down the rabbit hole into legal no man's land? Part 1", *ICCLR* 2018, Vol. 29, Issue 8, (483) 489-491; C. BROWN, T. DOLAN and K BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 76-77; M. NANNINGS, "Kwalificatie van crypto-assets als effect", *TFR* 2019/12, (623) 623-624.

49 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7.

50 See https://blog.bankera.com/2018/05/07/why-is-the-bnk-token-unique/.

51 See 2.7 Initial coin offerings: coins or tokens issued by an identifiable issuer, below.

52 S. BLEMUS and D. GUEGAN, "Initial Crypto-Asset Offerings (ICOs), Tokenization and Corporate Governance", January 2019, 8 (electronically available via https://ssrn.com/abstract=3350771).

53 A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", *TBH* 2019/2, (174) 182, footnote 103; M. NANNINGS, "Kwalificatie van crypto-assets als effect", *TFR* 2019/12, (623) 624.

54 S. BLEMUS and D. GUEGAN, "Initial Crypto-Asset Offerings (ICOs), Tokenization and Corporate Governance", January 2019, 9 (electronically available via https://ssrn.com/abstract=3350771).

55 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7.

56 See https://golem.network.

57 See https://filecoin.io.

58 A. SNYERS and K. PAUWELS, "ICOs in Belgium: down the rabbit hole into legal no man's land? Part 1", *ICCLR* 2018, Vol. 29, Issue 8, (483) 491.

their functional component[59].

Both investment and utility tokens can grant their holders certain governance rights in the issuing entity, such as the right to vote on distributions (investment tokens) or the right to vote for updates in the functional structure of the issuer's service (utility tokens)[60]. Once issued, both archetypes of tokens can be listed on secondary markets (so-called "crypto-exchanges"), where they can either be traded for fiat money or for other crypto-assets (usually cryptocurrencies)[61].

While it is theoretically feasible to draw a clear dividing line between cryptocurrencies and tokens, and, diving deeper into the latter category, investment and utility tokens, in practice it is not always easy to fit a crypto-asset into one or the other category[62]. This is because crypto-assets can exhibit features of more than one (sub-)category: they can embody a combination of an investment and/or a utility and/or a payment function. Crypto-assets that embody such a combination are commonly referred to as "hybrids" or "hybrid tokens"[63] and raise particular regulatory challenges[64]. An example of a hybrid token, more specifically an investment-utility hybrid, is Crypterium (CRPT)[65], which is used to pay transaction fees when using the services provided by the issuer (*i.e.* banking solutions), gives right to discounts for future services and gives a right to revenues[66].

[59] C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 77.

[60] F. ANNUNZIATA, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, 22-23 (electronically available via https://ssrn.com/abstract=3332485).

[61] M. NANNINGS, "Kwalificatie van crypto-assets als effect", *TFR* 2019/12, (623) 624.

[62] T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 27 and 29 (electronically available via https://ssrn.com/abstract=3337514).

[63] F. ANNUNZIATA, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, 21 and 25 (electronically available via https://ssrn.com/abstract=3332485); M. NANNINGS, "Kwalificatie van crypto-assets als effect", *TFR* 2019/12, (623) 624.

[64] See 4.4 Investments in crypto-assets, below.

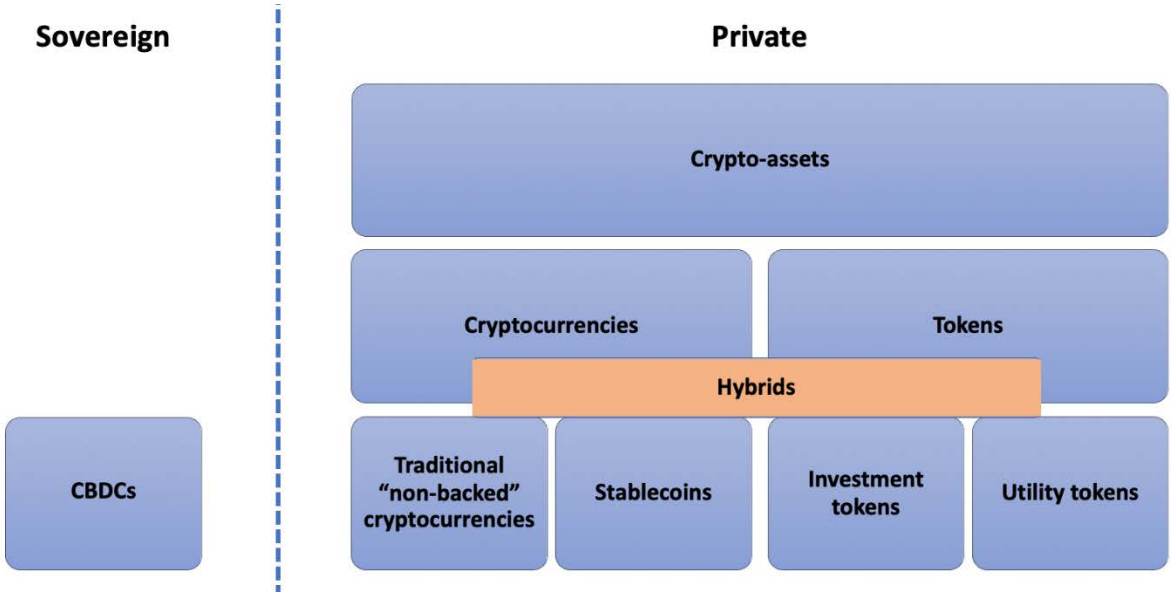
[65] See https://crypterium.com.

[66] See also T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 58 (electronically available via https://ssrn.com/abstract=3337514).

2.6. A taxonomy of crypto-assets

The observations set out above can be visually translated into the following taxonomy (see *Figure 1: Taxonomy of crypto-assets*).

Figure 1: Taxonomy of crypto-assets



Source: Figure 1 was created by the authors.

It should be noted that this taxonomy is not carved in stone. There are after all many ways to define the term "crypto-assets"[67]. Moreover, the above is a snapshot of what is out there now. The crypto-market continues to evolve, so what holds true today, may require an update in the future. That being said, by defining the overarching categories broadly, such as in this study, new sub-categories may be created thereunder.

2.7. Initial coin offerings: coins or tokens issued by an identifiable issuer

To conclude the introductory chapter on crypto-assets, it is relevant to analyse the phenomenon of initial coin offerings (ICOs).

In the beginning, the term ICO was primarily used to refer to a crowdsale organised upon the launch of a new cryptocurrency by a known or identifiable issuer[68]. The coin's inventors pre-mined a number

[67] *Cf.* D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 7 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf). E.g., if one would define it very narrowly, like the ECB Crypto-Assets Task Force does, then a distinction would have to be made between at least four "buckets" of "assets", side-by-side, namely 1) crypto-assets , 2) stablecoins, 3) tokens (or other assets) and 4) CBDCs. As discussed above, such approach is not instrumental to the scope of the research envisaged in this study. In addition, it does not adequately illustrate how the crypto-market has evolved up until now.

[68] See also: C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 77.

of coins and offered them to the public through a crowdsale to pay for development costs[69]. This was the case for Ethereum's ether (ETH) and Cardano's Ada (ADA)[70], amongst others.

Today, the term ICO is commonly used by regulatory authorities and legal scholars to refer to a process in which businesses (usually start-ups) or individuals issue tokens to the public to raise funds for their projects, in exchange for fiat money or other crypto-assets[71]. The term ICO, in this evolved meaning, is sometimes substituted for the term ITO (initial token offering) or token sale[72]. In legal literature, ICOs are typically compared to IPOs. Both are three-letter acronyms and both are aimed at raising money from the general public. There are, however, a number of differences between the two, aside from the instruments issued. Firstly, whereas a successful IPO generally requires the issuing companies to have a certain track-record, a successful ICO can be initiated at any stage. Secondly, IPOs typically involve a costly and time-consuming process. ICOs, on the other hand, can be launched through the issuer's website in a short period of time and generally do not require multiple actions from traditional intermediaries[73].

An ICO is typically preceded by a so-called "white-paper" made available on the issuer's website, in which the issuer describes his project, the tokens that will be issued and the technology and protocols underlying them[74]. The issuer will subsequently announce his project to the general public along with the date of the ICO through social media[75]. In order to subscribe to, hold and – at a later stage – trade tokens, investors will need to acquire a "digital wallet"[76]. Such wallet is also required to store and exchange other crypto-assets.

As indicated above, the words "initial coin offering" are currently used in a dual context to refer both to coins (cryptocurrencies) and tokens issued by an identifiable issuer. This is confusing. It makes sense to henceforth use the words "initial crypto-asset offering", which can also be abbreviated with the acronym ICO[77].

---

69 T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 9 (electronically available via https://ssrn.com/abstract=3337514).

70 See R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 34 and 41 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

71 See *inter alia* ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 11; EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7; F. ANNUNZIATA, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, 8 (electronically available via https://ssrn.com/abstract=3332485); CONGRESSIONAL RESEARCH SERVICE, "Digital Assets and SEC Regulation", January 2020, 5 (electronically available via https://www.hsdl.org/?view&did=833720).

72 See also A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", *TBH* 2019/2, (174) 175.

73 C. LE MOIGN, "ICO françaises: un nouveau mode de financement?", November 2018, 5 (electronically available via https://www.amf-france.org/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives?docId=workspace%3A%2F%2FSpacesStore%2F27604d2f-6f2b-4877-98d4-6b1cf0a1914b).

74 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 77.

75 T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 15 (electronically available via https://ssrn.com/abstract=3337514).

76 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 77.

77 See also S. BLEMUS and D. GUEGAN, "Initial Crypto-Asset Offerings (ICOs), Tokenization and Corporate Governance", January 2019, 7 (electronically available via https://ssrn.com/abstract=3350771).

3. STATE OF PLAY

3.1. Current markets

At the start of 2020, over 5,100 crypto-assets exist with a total market capitalisation exceeding $250 billion[78]. Recent data show that the crypto-market is still dominated by the cryptocurrency Bitcoin (BTC), with a dominance in terms of total market capitalisation exceeding 63% ($159 billion)[79]. The market capitalisation of privacy/anonymity-enhancing coins like Monero (XMR) and Dash (DASH)[80] has declined significantly at the end of 2018 and over the course of 2019. However, these coins remain popular, staying in the top 20 of coins in terms of market capitalisation, with daily trading volumes exceeding several million US Dollars[81].

Australian research published after our 2018 study *Cryptocurrencies and blockchain* suggests that $76 billion of illegal activity per year involves Bitcoin (amounting to 46% of all Bitcoin transactions); a number that comes very close to the US and EU markets for illegal drugs[82]. It highlights that both lawful and unlawful markets exist, where respectively legal and illegal users operate.

3.1.1. Lawful markets

Most legal activity in crypto-assets – and in particular in cryptocurrencies – takes place on crypto-exchanges. The research referred to above shows that legal users (those involved in legal activities) typically buy and hold cryptocurrencies as a speculative investment, rather than using them as a means of payment for goods or services offered by a legal merchant[83]. They also tend to hold larger balances than illegal users[84].

3.1.2. Unlawful markets

The legal activity in crypto-assets is but one half of the proverbial coin. The illegal activity, which includes, amongst others, the buying and selling of illegal goods or services (such as weapons, drugs and counterfeit documents) online in darknet marketplaces, money laundering, evasion of capital controls, payments in ransomware attacks and thefts, is just as significant. For example, the darknet marketplace Alphabay accepted payments in Bitcoin and the privacy-enhancing coin Monero, before it was seized by law enforcement agencies in the summer of 2017[85]. To give some idea as to just how significant the illegal activity is, reference can again be made to the research referred to above, which shows that almost half of all (yearly) transactions in Bitcoin can be linked to illegal activity[86]. Given Bitcoin's market share, this is an important observation. The research data also reveal that the average

---

78 Statement made on the basis of data derived from https://coinmarketcap.com on 4 March 2020.

79 Data derived from https://coinmarketcap.com on 4 March 2020.

80 R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 45 and 48 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

81 Data derived from https://coinmarketcap.com on 4 March 2020.

82 S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 26 (electronically available via https://ssrn.com/abstract=3102645).

83 S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 27 (electronically available via https://ssrn.com/abstract=3102645). See for a similar observation: G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.

84 S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 27 (electronically available via https://ssrn.com/abstract=3102645).

85 See A. GREENBERG, "Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire", https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.

86 S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 26 (electronically available via https://ssrn.com/abstract=3102645).

illegal user is involved in more transactions than the average legal user; tends to transact more, but uses smaller sized transactions; and, rather than hold onto Bitcoin for speculative purposes, tends to use his coins to buy and sell illegal goods and services[87]. The most important takeaway is thus that traditional coins, as a means of payment, are not so much used throughout the lawful economy, yet often throughout the unlawful economy.

Adding to this, other research found that despite the availability on the market of privacy/anonymity-enhancing coins like Dash and Monero, Bitcoin is still king[88]. Illegal users apparently keep resorting to third-party privacy/anonymity-enhancing services like mixers and tumblers (which obfuscate both the identifies of the sender and recipient of a coin) to conceal their crypto-transactions, rather than shift their focus entirely to privacy/anonymity-enhancing coins.

3.2. Central bank digital currencies and stable coins: game changers for (crypto) payments?

3.2.1. Central bank digital currencies (CBDCs)

During her first regular hearing as new president of the ECB in the ECON committee of the European Parliament, Ms. Christine Lagarde touched upon the topic of so-called central bank digital currencies (commonly abbreviated as CBDCs[89]), indicating that the ECB is playing its part in assessing whether they have any value for European citizens and the broader economy[90]. The ECB is far from the only central bank conducting such research. During the past couple of years, CBDCs have been studied by various central banks (and academics) across the world[91]. The research is still in full swing, but has gained a lot of momentum and increased media attention following the announcement of Facebook's Libra project on 18 June 2019[92].

a. To date: only private coins

To understand why central banks are looking into the issuance of their own digital currencies, one first has to understand that the digital payments landscape has evolved significantly during the last decade. After the emergence of Bitcoin in 2009, there have been numerous attempts to introduce a new "standard" for fast (international) payments.

Various tech-companies have entered the payment services market and big-tech (e.g. Facebook) has recently also jumped into the game coming up with its own plans for a new global payments scheme (e.g. the Libra) inspired by evolutions on the crypto-market[93].

---

87 S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 27 (electronically available via https://ssrn.com/abstract=3102645).

88 CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 34 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/).

89 Also see 2.3 Cryptocurrencies vs. central bank digital currencies: private vs. sovereign coins, above.

90 Introductory statement by Christine Lagarde, President of the ECB, at the ECON committee of the European Parliament, 2 December 2019, https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp191202~f8d16c9361.en.html.

91 Most research started in 2017, and the first reports appeared in 2018, see for example: CPMI, "Central bank digital currencies", March 2018, p. 34. (electronically available via https://www.bis.org/cpmi/publ/d174.pdf). See also C. BARONTINI and H. HOLDEN, "Proceeding with caution – a survey on central bank digital currency" (BIS Papers No 101), January 2019, https://www.bis.org/publ/bppdf/bispap101.pdf, 1.

92 See for example: https://www.reuters.com/article/us-eu-cryptocurrency-regulations/alarmed-by-libra-eu-to-look-into-issuing-public-digital-currency-draft-idUSKBN1XF1VC.

93 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 4 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

Up until now, initiatives to innovate the digital payments landscape have been private in nature and out of the central banks' grasp and sphere of influence, often even challenging their position. Together with the declining use of cash in a number of countries, this is a factor explaining why central banks are taking an interest in CBDCs[94].

b. Sovereign coins (or central bank digital currencies): the way of the future?

CBDCs, or sovereign coins, are not yet a reality (leaving some pilot programmes aside), but this could change in the near future.

i. What are CBDCs?

CBDCs can be designed in a number of ways[95]. As a result, there is no single definition of what constitutes a CBDC. Various definitions are put forward by international institutions and legal scholars, such as:

- "*a new form of digital central bank money that can be distinguished from reserves or settlement balances held by commercial banks at central banks*"[96];
- "*a central bank money denominated in the official unit of account for general purpose users that can be exchanged, peer-to-peer, in a decentralised manner*"[97];
- "*a digital asset issued by a central bank for the purpose of payment and settlement, in either retail or wholesale transactions*"[98]; and
- "*some form of central bank money handled through electronic means and accessible to the broad public*"[99].

At the most basic level, a CBDC can be described as "***monetary value stored electronically that represents a liability of the central bank and can be used to make payments***"[100].

CBDCs should not be mistaken for crypto-assets[101]. The research into CBDCs may have been triggered by the emergence of crypto-assets, and in particular cryptocurrencies, but the two are different from each other. First of all, whereas crypto-assets are private assets, CBDCs are sovereign in nature. Secondly, whereas the issuance of crypto-assets relies on the use of DLT or similar technology, the issuance of CBDCs is not contingent upon the use of any specific technology[102]. DLT and cryptography

---

94 See also H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 117; C. CALCATERRA, W. A. KAAL and V. RAO, "Stable cryptocurrencies – First Order Principles", *Stanford Journal of Blockchain Law & Policy (2019)*, June 2019, 11-12 (electronically available via https://ssrn.com/abstract=3402701); CPMI, "Central bank digital currencies", March 2018, 3 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

95 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 32 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

96 CPMI, "Central bank digital currencies", March 2018, 1 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

97 H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 117.

98 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 2 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

99 U. BINDSEIL, "Central bank digital currency - financial system implications and control", July 2019, 2 (electronically available via https://ssrn.com/abstract=3385283).

100 W. ENGERT and B. S. C. FUNG, "Central Bank Digital Currency: Motivations and Implications", *Bank of Canada Staff Discussion Paper*, November 2017, 1-2 (electronically available via https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf); H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 117.

101 See also 2.3 Cryptocurrencies vs. central bank digital currencies: private vs. sovereign coins, above.

102 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 32 (electronically available via

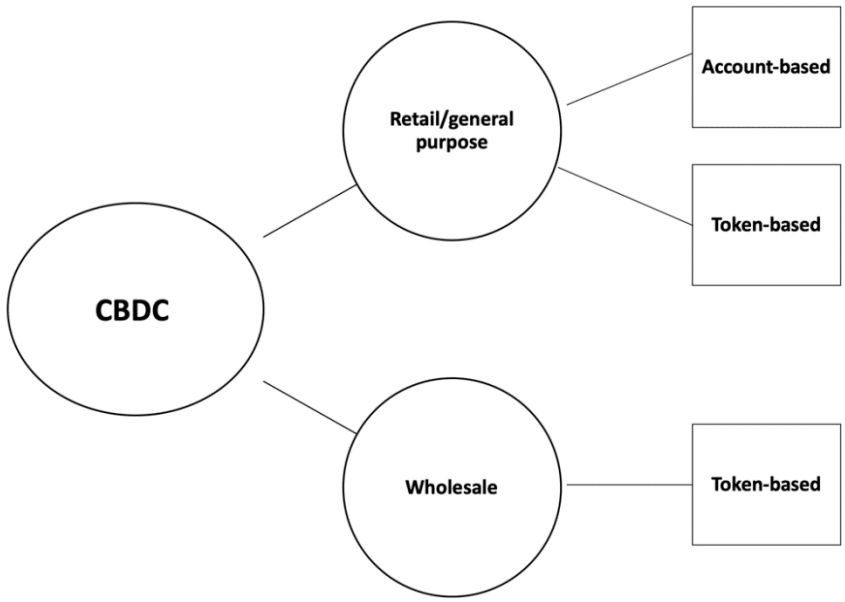
may be used, but for many central banks it remains unclear whether they are the best route forward for digital currency implementation[103]. Thirdly, whereas crypto-assets, most notably cryptocurrencies, lack the status of legal currencies, the opposite would be true for CDBCs[104]. CBDCs are envisioned by most to be a new form of central bank *money*[105].

In its 2018 report on CBDCs, the CPMI has indicated there are various design choices for a CBDC. The most important ones are: 1) access (widely or restricted); 2) degree of anonymity (ranging from complete to none); 3) operational availability (ranging from current opening hours to 24 hours a day and seven days a week); and 4) interest bearing characteristics (yes or no)[106].

ii. Imaginable forms

Given the different design choices to be made, many forms of CBDCs are imaginable. Most legal scholars and central banks typically distinguish two main types of CBDCs: "retail" or "general purpose" CBDCs on the one hand and "wholesale" CBDCs on the other hand[107]. Both types can be further delineated as illustrated in *Figure 2: Main types of CBDCs* below.

Figure 2: Main types of CBDCs



Source: Figure 2 was created by the authors. Its content is based on the 2018 CPMI study titled "Central bank digital currencies"[108].

https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf); D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 8 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

[103] OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 35 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf). See to the contrary: H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 117.

[104] H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 119.

[105] CPMI, "Central bank digital currencies", March 2018, 3 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

[106] See CPMI, "Central bank digital currencies", March 2018, 1 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

[107] H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 117; U. BINDSEIL, "Central bank digital currency - financial system implications and control", July 2019, 2 (electronically available via https://ssrn.com/abstract=3385283); CPMI, "Central bank digital currencies", March 2018, 4 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

[108] See CPMI, "Central bank digital currencies", March 2018, 1 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

The main difference between retail and wholesale CBDCs is that first type would be accessible to all households and would be primarily targeted at retail transactions, while the second type would only be accessible to certain agents and specifically targeted at interbank payments and settlements[109].

Theoretically, retail CBDCs could be implemented in one of the two following formats:

- Firstly, retail CBDCs could be offered to all households and corporates in the form of **deposit accounts** at the central bank[110]. Such accounts are not a "new" creation. They already exist today, but are only available to commercial banks and certain institutions (e.g., governments and financial market infrastructures), who can hold reserves at the central bank[111]. The real novelty of a retail "account-based" CBDC would be the decision to also implement them for the general public.

- Alternatively, retail CBDCs could be offered in the form of **tokens of stored value** that would circulate in a decentralised manner without a central ledger[112]. The term "tokens" is used here within its payment economics meaning to clarify the difference with an account-based format; it does not refer to and should not be mistaken for the subcategory of crypto-assets referred to above[113]. After all, CBDCs do not classify as crypto-assets.

  A retail "token-based" CBDC, sometimes also referred to as a retail "value-based" CBDC, would be a type of "digital or digitalised cash" issued by the central bank for the general public[114]. It would likely be complementary to banknotes, coins, and wholesale deposits provided by the central bank, and to commercial bank deposits and electronic money (e-money) provided by private entities under the relevant licensing regimes[115].

  In payment economics, a key difference between a "token- (or value-) based" instrument and an "account-based" instrument is in its verification. A person receiving a "token" will have to verify that the "token" is genuine. A person receiving payment through an "account-based" instrument will not have to make such verification: the party where the account is held will verify the identity of the account holder(s)[116].

Wholesale CBDCs (for interbank payments and settlements) would most likely be offered in the form of tokens of stored value[117]. An implementation in the form of deposit accounts at the central bank would not make much sense, as the agents that would have access to such a wholesale CBDC already have access to central bank accounts today (*i.e.* reserves and settlement accounts[118]). A wholesale

---

109 U. BINDSEIL, "Central bank digital currency - financial system implications and control", July 2019, 6 (electronically available via https://ssrn.com/abstract=3385283).

110 *Ibidem*, 2.

111 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 32 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

112 U. BINDSEIL, "Central bank digital currency - financial system implications and control", July 2019, 2 (electronically available via https://ssrn.com/abstract=3385283).

113 See 2.5 Tokens can be investment tokens or utility tokens or hybrid forms thereof.

114 H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 118.

115 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 32 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

116 C. BARONTINI and H. HOLDEN, "Proceeding with caution – a survey on central bank digital currency" (BIS Papers No 101), January 2019, https://www.bis.org/publ/bppdf/bispap101.pdf, 2.

117 CPMI, "Central bank digital currencies", March 2018, 1, 4 and 8 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

118 *Ibidem*, 4.

"token-based" CBDC would not be used as a digital extension of cash like its retail counterpart, but would serve as a settlement asset in the interbank market[119].

iii. Pros and cons

Research shows that there are both benefits and risks attached to the introduction of CBDCs.

Table 1: Overview of benefits and risks commonly associated with CBDCs provides an overview of the benefits and risks that are typically brought forward by legal scholars and central banks, in particular in relation to retail CBDCs which are considered to be the most innovative type of CBDCs. The overview is high-level and not intended to be exhaustive.

Table 1: Overview of benefits and risks commonly associated with CBDCs

Benefits	Comments
Efficient retail payments	In jurisdictions where the use of cash is (rapidly) declining, CBDCs could serve as an alternative safe, robust and convenient payment instrument for use by the general public[120]. The issuance thereof would guarantee that citizens retain access to the central bank balance sheet[121]. CBDCs could also provide 24/7 access to payments with instant settlement[122].
Better control of illicit payment and saving activities, money laundering, and terrorist financing	Depending on the design and implementation choices made (*i.e.* CBDCs not taking the form of anonymous token money), CBDCs could allow for a better monitoring of payment flows and help improve anti-money laundering and counter terrorist financing enforcement, compared to cash[123].
Financial inclusion	CBDCs have the potential to improve financial inclusion and help bank the unbanked. Recent research shows that many unbanked individuals are discouraged by high bank fees on accounts and transfers and that making digital payments infrastructure publicly available through a CBDC would offer a cost-efficient alternative[124].
Additional monetary policy tool	According to the CPMI, CBDCs could enrich the options offered by the central bank's monetary policy toolkit (for example by allowing for a strengthening of pass-through of policy rate changes to other interest rates or addressing the zero-lower bound (or the even lower, effective bound) on interest rates)[125].

[119] OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 2 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

[120] CPMI, "Central bank digital currencies", March 2018, 1 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

[121] U. BINDSEIL, "Central bank digital currency - financial system implications and control", July 2019, 3 (electronically available via https://ssrn.com/abstract=3385283).

[122] OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 16 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

[123] U. BINDSEIL, "Central bank digital currency - financial system implications and control", July 2019, 2 (electronically available via https://ssrn.com/abstract=3385283).

[124] OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 20 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

[125] CPMI, "Central bank digital currencies", March 2018, 2 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

Risks	Comments
Structural disintermediation of banks	The CPMI has pointed out that the introduction of CBDCs could result in a wider presence of central banks in financial systems. This could mean a greater role for central banks in allocating economic resources, which could potentially lead to overall economic losses should such entities be less efficient than the private sector in allocating resources[126]. Another concern is that there may also be greater political interference.
"Digital runs" towards the central bank	Retail CBDCs could have destabilising effects in the event of a financial crisis. During a systemic banking crisis, holding a risk-free CBDC could become a lot more attractive than commercial bank deposits. This could eventually result in a sector-wide run on commercial bank deposits, magnifying the effects of the crisis[127]. Money could easily be moved out of the commercial banking sector, which could, in turn, impact the flow of credit to the economy[128].

iv. What's inside the lab?

Now that the research on CBDCs is reaching its zenith, it is interesting to explore what is inside the lab. Just outside of the euro area, the *Sveriges Riksbank* (the Swedish central bank) has been working on a retail CBDC project, the "e-krona", which is motivated by the declining use of cash in Sweden. It started the project in the beginning of 2017[129] and is now preparing to launch a pilot programme[130]. The research on the e-krona project has so far produced two extensive reports which can be consulted on the *Sveriges Riksbank* 's website[131].

Outside Europe, in Uruguay, the Central Bank of Uruguay has already successfully closed a small-scale pilot programme on a retail CBDC, the "e-peso". The programme was launched in late 2017. Individual users and businesses who were selected to participate in the project could hold e-pesos in mobile electronic wallets. E-pesos could be transferred instantly, peer-to-peer, via mobile phones using either text messages or a specific e-peso app. Interesting to note is that the pilot programme did not make use of DLT[132]. All e-pesos were cancelled after the closing of the pilot programme and the Central Bank of Uruguay is now evaluating the project[133].

In February 2018, another digital state currency popped up in South-America with the Venezuela-government issuing the "Petro", hoping to counter the hyperinflation of its national currency, the bolivar, and hoping to minimise the effects of international financial sanctions taken against the country[134]. The project got a lot of media attention, but failed massively due to the poor quality of the

---

126 *Ibidem*.

127 U. BINDSEIL, "Central bank digital currency - financial system implications and control", July 2019, 15 (electronically available via https://ssrn.com/abstract=3385283).

128 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 30 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

129 CPMI, "Central bank digital currencies", March 2018, 3 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

130 Sweden's central bank says to launch digital currency pilot project, December 2019, https://www.reuters.com/article/sweden-centralbank/swedens-central-bank-says-to-launch-digital-currency-pilot-project-idUSL8N28N463.

131 See https://www.riksbank.se/en-gb/payments--cash/e-krona/.

132 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 20 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

133 CPMI, "Central bank digital currencies", March 2018, 5 (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).

134 I. H. ANCHUSTEGUI and T. S. HUNTER, "Oil as Currency: Venezuela's Petro, a New 'Oil Pattern'?", November 2018, 1, 11 and 17 (electronically available via https://ssrn.com/abstract=3291272); S. J. HUGHES, "'Gatekeepers' Are Vital Participants in Anti-Money- Laundering Laws and Enforcement Regimes as Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to 'Follow the Money'",

information presented to the public and overall misinformation[135]. For example, the Petro was announced as an oil-backed digital asset (backed 1:1 by barrels of Venezuelan oil), but this turned out to be a hoax[136].

Another example of a CBDC project that is apparently well on its way is that of the People's Bank of China, which is reportedly already performing closed-loop testing simulating various payment scenarios[137].

Inside the euro area, the Governor of the *Banque de France* recently announced that the *Banque de France* is keen to start running its own CBDC experiments and will launch a call for projects before the end of the first quarter of 2020[138]. Its initial focus will be on a wholesale type of CBDC.

Will we also see a full-fletched "e-euro" project in the short- to mid-term? According to the ECB Crypto-Assets Task Force the business case for issuing a CBDC in the euro area is currently not compelling. It points out that:

- even though non-cash payments in the EU continue to grow every year, the demand for euro banknotes has been sustained, and cash is generally still a popular means of payment across the euro area;
- European citizens and companies currently already have access to a wide array of electronic payment instruments that work well and are underpinned by sound clearing and settlement infrastructures;
- instant payments have already become a reality, making it easy to match the speed of a cash payment in the digital economy; and
- the euro area's TIPS (TARGET Instant Payments Settlement) service, which was introduced in November 2018, already enables real-time settlement in central bank money on a 24/7/365 basis[139].

Hence, it is considered that the modernisation of existing retail and wholesale payment systems currently suffices and does not warrant the issuance of a CBDC in the euro area. This could, however, change in the future. To remain up to speed, the ECB is working closely together with other European central bank community members in the context of the so-called "EUROchain" research network. In December 2019, researchers active within this network published a paper exploring anonymity in CBDCs, presenting a proof of concept for anonymity in digital cash[140]. While extremely interesting, the

Indiana Legal Studies Research Paper No. 408 (2019), August 2019, 8-9 (electronically available via https://ssrn.com/abstract=3436098); CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 29 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/).

135 B. ELLSWORTH, "Special Report: In Venezuela, new cryptocurrency is nowhere to be found", August 2018, https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U?utm_source=MIT+Technology+Review&utm_campaign=e648089a9e-EMAIL_CAMPAIGN_2018_02_27_COPY_02&utm_medium=email&utm_term=0_997ed6f472-e648089a9e-157724665.

136 See D. FLOYD, "Venezuela's Petro Isn't Oil-Backed. It's Not Even a Cryptocurrency (Opinion)", June 2019, https://www.investopedia.com/news/venezuela-petro-not-cryptocurrency/. See also I. H. ANCHUSTEGUI and T. S. HUNTER, "Oil as Currency: Venezuela's Petro, a New 'Oil Pattern'?", November 2018, 13-15 (electronically available via https://ssrn.com/abstract=3291272).

137 See C. JIA, "China's digital currency may be world first", 9 September 2019, https://www.telegraph.co.uk/china-watch/technology/china-digital-currency/.

138 F. VILLEROY DE GALHAU, "Speech on Central bank digital currency and innovative payments", December 2019, 4 (electronically available via https://www.banque-france.fr/sites/default/files/medias/documents/2019.12.04_conference_acpr_en_v5.pdf).

139 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 33 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

140 ECB, "Exploring anonymity in central bank digital currencies", *In Focus Issue No 4*, December 2019, p. 11. (electronically available via https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf).

research it is not geared towards practical implementation and does not imply any decision to proceed with a CBDC in the foreseeable future.

Box 1: CBDCs can be anonymous and AML/CFT compliant

Replacing anonymous, untraceable cash with a public, traceable CBDC, could theoretically mark the end of many money laundering and criminal activities. However, it is unlikely that this scenario will get the required political backing any time soon. The reason is simple: the general public still uses a lot of cash and many people have strong feelings about the privacy it provides them. They do not want central banks and government authorities to have insight into all details of their payment transactions. The challenge for central banks is thus to design and implement a CBDC that strikes a balance between this demand for user integrity, and the need to comply with AML/CFT standards.

The aforementioned EUROchain research network has recently made a remarkable effort to find such balance. It has developed a proof of concept for anonymity in digital cash, more in particular a token-based variant of CBDC with cash-like features. In short, EUROchain's proof of concept provides a digitalisation solution for AML/CFT compliance procedures whereby a user's identity and transaction history cannot be seen by the central bank or intermediaries other than those chosen by the user. The enforcement of limits on anonymous electronic transactions is automated, and additional AML/CFT checks are delegated to a dedicated AML authority, which checks the identities of users involved in large-value transactions and prevents CBDC from being transferred to embargoed users. All of this is technically achieved using "anonymity vouchers", which allow users to anonymously transfer a limited amount of CBDC over a defined period of time. Further details on the concept can be found in the December 2019 EUROchain report presented by the ECB (*Focus Issue No 4*, referred to above).

All in all, as it stands, it is still too early to tell whether CBDCs will indeed be(come) game changers for payments. More research needs to be done. At the time of writing, the Bank of Canada, the Bank of England, the Bank of Japan, the ECB, the Sveriges Riksbank and the Swiss National Bank, have just set up a working group together with the BIS, to share experiences. According to a press release made upon the announcement of the working group, the group will assess CBDC use cases, economic, functional and technical design choices, including cross-border interoperability, and share knowledge on emerging technologies[141]. Exiting times are ahead for central bankers and regulators alike.

3.2.2. Stablecoins

The year 2019 will probably not go into the history books as the year in which the interest in CBDCs peaked, but rather as the year the general public became acquainted with Facebook's Libra project and the concept of so-called "stablecoins".

[141] BIS, "Central bank group to assess potential cases for central bank digital currencies", 21 January 2019, https://www.bis.org/press/p200121.htm.

a. The early day coins are not used as a means of payment because of volatility

To understand what "stablecoins" are all about, and how they differ from popular cryptocurrencies or coins like Bitcoin, Litecoin or Bitcoin Cash, it is important to recall that those who created the very first cryptocurrencies did so with the intention to create a new means of payment for use by the general public[142]. However, things have turned out differently. The early day coins have not evolved into a new means of payment or store of value, but have served more as a highly speculative asset class for certain investors[143]. As aforementioned, research suggests that those who do use coins like Bitcoin as a means of payment, primarily do so for illegal purposes on illegal markets[144].

The main reason the early day coins, also referred to as the first wave of cryptocurrencies, are not used as a means of payment, is because their value, *i.e.* the price at which they are traded, is highly volatile[145]. They are not backed by, or based on, any underlying asset, claim or liability, and this makes them prone to serious fluctuations[146].

Coins that fail to hold a steady or stable value generally fail to function both as a medium of exchange, a unit of account and a store of value, *i.e.* the three indicia of money[147].

b. The story of stablecoins to overcome the problem of volatility

To overcome the problem of volatility, a number of players on the crypto-market came up with the idea to develop a new type of cryptocurrency[148]. Interestingly enough, their primary aim was not to create a new crypto-asset capable of performing all three functions of money (this was more of a secondary aim), but to protect revenues earned from crypto-asset investments from serious price drops, and, hence, to hedge against market movements[149]. The asset that was ultimately created is now commonly referred to as a "stablecoin".

---

142 A. ADIMI GIKAY, "Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons From European Union Law", *9 Case Western Reserve Journal of Law, Technology & the Internet 1 (2018)*, March 2018, 5 (electronically available via https://ssrn.com/abstract=3142317); T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 20 (electronically available via https://ssrn.com/abstract=3337514).

143 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1. See also C. CALCATERRA, W. A. KAAL and V. RAO, "Stable cryptocurrencies – First Order Principles", *Stanford Journal of Blockchain Law & Policy (2019)*, June 2019, 20 (electronically available via https://ssrn.com/abstract=3402701).

144 See 3.1.2 Unlawful markets.

145 D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 4 (electronically available via https://ssrn.com/abstract=3414401).

146 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 8 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

147 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 6 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf); H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 113.

148 I. G.A. PERNICE, S. HENNINGSEN, R. PROSKALOVICH, M. FLORIAN, H. ELENDNER and B. SCHEUERMANN, "Monetary Stabilization in Cryptocurrencies—Design Approaches and Open Questions", June 2019, 1 (electronically available via https://ssrn.com/abstract=3398372); D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 6 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

149 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 14 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf); D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 6 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

i. What are stablecoins?

Just like the term CBDC, the term "stablecoin" does not have an agreed definition. Various definitions of stablecoins are put forward by legal scholars and international institutions, such as:

- "*a new class of cryptocurrencies which offer price stability and/or are backed by reserve asset(s), [combining] the instant processing and security of payments of cryptocurrencies, and the volatility-free stable valuations of fiat currencies*"[150];
- "*digital units of value that are not a form of any specific currency (or basket thereof) but rely on a set of stabilisation tools which are supposed to minimise fluctuations of their price in such currency(ies)*"[151];
- "*coins that represent a claim, either on a specific issuer or on underlying assets or funds, or some other right or interest*"[152];
- "*a variant of cryptocurrencies typically pegged to the price of another asset (such as the dollar), designed to maintain a stable market value*"[153]; and
- "*crypto-assets designed to maintain a stable value relative to another asset (typically a unit of currency)*"[154].

At the most basic level, stablecoins can be described as a new type of cryptocurrencies that is not just perceived as something of value by its users, but is actually backed by something of value[155]. Unlike CBDCs, stablecoins are not just a lab experiment; various examples are already in circulation.

Stablecoins are a new phenomenon, but not as new as one might think. The first stablecoin, Tether (USDT) already dates back from 2014[156]. Other stablecoin projects like Gemini Dollar (GUSD) and Paxos Standard (PAX)[157] are more recent, but nevertheless already nearing their second birthday.

Unlike most traditional "non-backed" cryptocurrencies[158], stablecoins typically have an identifiable issuer, or require the intervention of third-party accountable institutions (e.g., custodians) that can be held responsible by regulators and users[159]. However, there are also stablecoins where the link with a liable party cannot be so easily made[160].

---

150 C. CALCATERRA, W. A. KAAL and V. RAO, "Stable cryptocurrencies – First Order Principles", *Stanford Journal of Blockchain Law & Policy (2019)*, June 2019, 2 (electronically available via https://ssrn.com/abstract=3402701).

151 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 9 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

152 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.

153 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 2 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

154 FSB, "Crypto-assets: work underway, regulatory approaches and potential gaps", May 2019, https://www.fsb.org/wp-content/uploads/P310519.pdf, 10.

155 See also 2.4 Cryptocurrencies can be backed ("stable") or not, above.

156 C. CALCATERRA, W. A. KAAL and V. RAO, "Stable cryptocurrencies – First Order Principles", *Stanford Journal of Blockchain Law & Policy (2019)*, June 2019, 2 (electronically available via https://ssrn.com/abstract=3402701).

157 See https://www.paxos.com/pax/.

158 See R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 67 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

159 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.

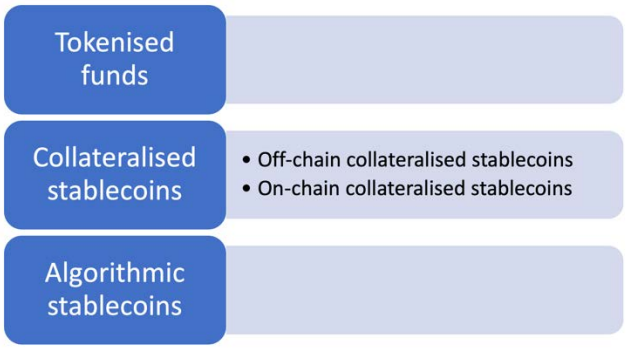
160 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 10 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

Like traditional "non-backed" cryptocurrencies, stablecoins are crypto-assets[161]. They are private and digital in nature and they use DLT, often an existing blockchain.

ii. Stablecoin types

As their name suggests, stablecoins make use of so-called "stabilisation mechanisms". Their value is backed or underpinned by "something" allowing them to maintain a stable value. Depending on what this something is, they can be further delineated into three broad categories[162], as visually illustrated in *Figure 3: Stablecoin types below*. Other classifications are also possible, but are a lot more technical and go beyond the scope of this study[163].

Figure 3: Stablecoin types



Source: Figure 3 was created by the authors. Its content is based on ECB Occasional Paper Series No. 230 by D. BULLMANN, J. KLEMM and A. PINNA[164].

The first category of stablecoins that can be distinguished, is the category that is *supported by funds*, sometimes also referred to as "tokenised funds" or the "depository receipt model"[165]. It relates to units of monetary value that are stored electronically in a distributed ledger to represent a claim on an issuer, usually a legal entity, and are issued, on receipt of funds, for the purpose of making payment transactions to persons other than the issuer[166]. The issuer holds the funds or involves a custodian for that purpose, and ensures that the funds backing the stablecoins are redeemable (at par value).

The second category of stablecoins that can be distinguished, is the category that is *supported by an asset or multiple assets other than funds* against which users can redeem their holdings. The coins that fall within this category are referred to as a "collateralised stablecoins" and, broadly speaking, come in two variants:

---

[161] See also 2.4 Cryptocurrencies can be backed ("stable") or not, above.

[162] D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 10 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

[163] See for example I. G.A. PERNICE, S. HENNINGSEN, R. PROSKALOVICH, M. FLORIAN, H. ELENDNER and B. SCHEUERMANN, "Monetary Stabilization in Cryptocurrencies—Design Approaches and Open Questions", June 2019, 12 (electronically available via https://ssrn.com/abstract=3398372).

[164] D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 10 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

[165] G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 24.

[166] D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 12 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

- The first variant is *supported by traditional assets*, such as commodities and real estate, and typically requires a custodian for safekeeping[167]. The coins that fall within this category are called "off-chain collateralised stablecoins";
- The second variant is *supported by assets in digital form*, typically other crypto-assets. They can be held in a decentralised manner[168]. The coins that fall within this category (like Multi-collateral DAI (DAI)) are called "on-chain collateralised stablecoins".

Coins can also be stabilised with collateral by linking their value to a basket of reference assets. Such basket can include commodities and real estate, but also government securities and fiat currencies. The stabilisation mechanism usually works much like an exchange-traded fund, where the holder does not own the underlying assets[169], yet other technical implementations are also possible.

The third category of stablecoins is a bit of an odd one out, as it is *supported solely by users' expectations about the future purchasing power of their holdings*[170]. The coins that fall within this category are often referred to as "algorithmic stablecoins"[171]. They seek to maintain par value with a currency of reference through algorithmic trading, *i.e.* by automatically adjusting the supply of stablecoin units[172]. Algorithmic stablecoins do not require the accountability of any party, nor the custody of any underlying asset[173]. With the exception of NuBits[174], which failed to deliver on the promise of stability, their advent is still largely theoretical. Most initiatives are still in the development phase.

Just like CBDCs, stablecoins can be for retail or for wholesale purposes, which means they can either be used by anyone, or only by a select number of actors[175]. Most stablecoin initiatives currently on the market are for retail purposes. An example of a wholesale stablecoin is JPM Coin[176].

iii. What do the numbers tell?

According to research carried out in 2019 at the request of the ECB, the overall market capitalisation of stablecoins almost tripled from €1.5 billion in January 2018 to more than €4.3 billion in July 2019, with average transaction volumes of €13.5 billion per month between January and July 2019[177]. Out of more than fifty stablecoin initiatives identified, the bulk of which still in development, tokenised funds were found to be the most common stablecoin type, followed by on-chain collateralised stable-coins. What

---

167 *Ibidem*, 10.

168 *Ibidem*, 10.

169 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 24.

170 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 10 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

171 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 10 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf); G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 24.

172 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 26 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

173 *Ibidem*, 10.

174 See https://nubits.com.

175 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1 and 24.

176 See https://www.jpmorgan.com/global/news/digital-coin-payments.

177 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 31 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).

is interesting is that nearly half of all initiatives identified was said to make use of the Ethereum DLT network[178].

Most stablecoin initiatives are pegged to the US Dollar. However, there are also stablecoins that seek to maintain a par value (1:1) with the euro. One of the largest stablecoins "tokenising" the euro is STASIS EURO (EURS)[179]. Its market capitalisation, at the time of writing, amounts to $35,69 million[180] (*i.e.* €32.08 million).

Even though their market capitalisation has grown significantly over the last two years, stablecoins are still a marginal phenomenon in the world of crypto-assets. For instance, if one compares their overall market capitalisation to that of the first wave of cryptocurrencies, like Bitcoin and Litecoin, this still comes nowhere near[181]. However, given the growing interest in these coins, that could change quickly.

c. Global and local stablecoins

Although most stablecoins can be traded on one or more crypto-exchanges on a 24/7 basis, from nearly anywhere in the world, they have yet to reach a very wide user base. Their actual footprint usually does not reach further than a few jurisdictions. In other words, their impact remains local.

Recently, new stablecoin initiatives have emerged. The most important one is probably Facebook's Libra project. These new initiatives that are built on top of existing, large and/or cross-border user bases. They have the potential to scale very quickly to achieve a global or other substantial footprint[182] and are commonly referred to as "global stablecoins"[183]. Global stablecoins are currently under a lot of scrutiny, because they could pose significant risks to financial stability and monetary policy[184].

d. Libra

On 18 June 2019, social media giant Facebook officially announced that it was planning to issue its own global cryptocurrency under the name "Libra" in the first half of 2020[185]. Its plans immediately came to the attention of several prominent financial regulators who did not need much time to voice serious concerns on the potential regulatory impact of the project considering Facebook's vast user base and global reach[186]. Facebook was urged to put the actual issuance of the coin on hold until all regulatory concerns are addressed and in July 2019 it confirmed it would do so[187].

---

178 *Ibidem*, 32.

179 See https://eurs.stasis.net.

180 Data derived from https://coinmarketcap.com on 4 March 2020.

181 If one looks at coins individually, the story is a lot more nuanced. For example, the very first stablecoin, Tether (USDT) currently has a total market capitalisation of $4.64 billion and takes the "top 5" spot of all cryptocurrencies in terms of total market capitalisation (according to data derived from https://coinmarketcap.com on 4 March 2020).

182 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 2.

183 FSB, "Regulatory issues of stablecoins", October 2019, https://www.fsb.org/wp-content/uploads/P181019.pdf, 1; G20, "Press Release on Global Stablecoins", October 2019, https://www.boj.or.jp/en/announcements/release_2019/data/rel191021e1.pdf, 1; IOSCO, "Statement on IOSCO study of emerging global stablecoin proposals", November 2019, https://www.iosco.org/news/pdf/IOSCONEWS550.pdf, 1.

184 See 4.1.1 Concern: global stablecoins as a threat to financial stability and monetary policy, below.

185 See LIBRA, "Whitepaper: An introduction to Libra", June 2019, https://libra.org/en-US/white-paper/#introducing-libra, p. 12.

186 D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 3 (electronically available via https://ssrn.com/abstract=3414401). See also CONGRESSIONAL RESEARCH SERVICE, "Digital Assets and SEC Regulation", January 2020, 14-15 (electronically available via https://www.hsdl.org/?view&did=833720).

187 See B. BAIN and A. WEINSTEIN, "Facebook Says Libra Won't Launch Until Regulators Satisfied", July 2019, https://www.bloomberg.com/news/articles/2019-07-15/facebook-says-libra-won-t-launch-until-regulators-satisfied. See also 4.1.2 G20 approach: no global private stablecoins before a sufficient regulatory regime is in place, below.

i. What is Libra?

Libra, as it is envisaged, is a global, collateralised stablecoin. According to Libra's whitepaper, its value will be fully backed by a reserve of real assets comprised of a basket of bank deposits and short-term government securities[188] in currencies from stable and reputable central banks, most likely the dollar, euro, renminbi, yen and pound[189].

Libra is a stablecoin and thus by extension also a cryptocurrency and a crypto-asset. It is built on the foundation of blockchain technology, more in particular the "Libra Blockchain"[190]. Using blockchain technology, Libra wants to make moving money around as easy and cost-effective as sending a text message or sharing a photo, no matter where you live, what you do, or how much you earn. The idea is that Libra will be a simple global currency and financial infrastructure that will empower billions of people[191]. One of its selling points is that it will help bank those who are currently "unbanked" and, thus, will effectively promote financial inclusion[192].

ii. How does Libra work?

Without going into all the details and technicalities and merely descriptive, the Libra scheme functions as follows. In short, to start using Libra, people will first have to acquire units of Libra with fiat currency. Similar to how other cryptocurrencies are acquired, they will have to go to an authorised exchange to that end. To hold and store Libra, Libra users will most likely be required to have a Libra account or a Libra wallet at a Libra custodian or an authorised exchange[193]. Authorised exchanges will match users' Libra demand by (i) selling units of Libra from their own Libra supply, (ii) buying Libra from other Libra users in return for fiat currency (*i.e.* from those users who want to cash-out) or (iii) request additional Libra from the Libra Association. Holders of Libra will only have a non-secured claim to exchange their Libra for local fiat currency at a value reflecting the value of assets in the Libra reserve, which may fluctuate[194]. They will not have a direct claim on the Libra reserve, which means that if the reserve were to be liquidated, they will lose out[195].

The Libra Association, a not-for-profit membership organisation based in Geneva, Switzerland, will be the only entity that can create and destroy Libra. It will govern the Libra blockchain and manage the Libra reserve[196]. The Libra Association serves to distance Facebook from the Libra project and will consist of diverse members who will operate the nodes validating Libra transactions[197]. Libra will be

---

188 See LIBRA, "Whitepaper: An introduction to Libra", June 2019, https://libra.org/en-US/white-paper/#introducing-libra, 3.

189 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 11 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf); V. BRÜL, "Libra – A Differentiated View on Facebook's Virtual Currency Project", *Intereconomics 2020/1 (ZBW – Leibniz Information Centre for Economics)*, 54.

190 See on the Libra Blockchain: Z. AMSDEN, R. ARORA, S. BANO, M. BAUDET, S. BLACKSHEAR, A. BOTHRA, G. CABRERA, C. CATALINI, K. CHALKIAS, E. CHENG, A. CHING, A. CHURSIN, G. DANEZIS, G. DI GIACOMO, D. L. DILL, H. DING, N. DOUDCHENKO, V. GAO, Z. GAO, F. GARILLOT, M. GORVEN, P. HAYES, J. M. HOU, Y. HU, K. HURLEY, K. LEWI, C. LI, Z. LI, D. MALKHI, S. MARGULIS, B. MAURER, P. MOHASSEL, L. DE NAUROIS, V. NIKOLAENKO, T. NOWACKI, O. ORLOV, D. PERELMAN, A. POTT, B. PROCTOR, S. QADEER, RAIN, D. RUSSI, B. SCHWAB, S. SEZER, A. SONNINO, H. VENTER, L. WEI, N. WERNERFELT, B. WILLIAMS, Q. WU, X. YAN, T. ZAKIAN and R. ZHOU, "The Libra Blockchain", September 2019, https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf, p. 29.

191 See LIBRA, "Whitepaper: An introduction to Libra", June 2019, https://libra.org/en-US/white-paper/#introducing-libra, 3.

192 D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 11 (electronically available via https://ssrn.com/abstract=3414401).

193 *Ibidem*, 5.

194 See LIBRA, "Whitepaper: An introduction to Libra", June 2019, https://libra.org/en-US/white-paper/#introducing-libra, 7.

195 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 11 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).

196 See LIBRA, "Whitepaper: An introduction to Libra", June 2019, https://libra.org/en-US/white-paper/#introducing-libra, 8.

197 *Ibidem*.

established as a permissioned system [198]: only the members of the Libra Association will be allowed to operate nodes and participate in transaction validation [199].

Contrary to cryptocurrencies like Bitcoin, Libra will not be a fully decentralised system. As a central governing body, the Libra Association will function as the final decision-making authority[200].

To implement a separation between social and financial data – Libra will, after-all, be used by Facebook users – Facebook has also created a new subsidiary named "Calibra" to build and operate services on its behalf on top of the Libra network [201].

iii. Libra's launch is currently on hold, but regulators have not been idle

Libra is not here yet, and given the regulatory concerns surrounding the project (see below[202]), it will probably still take a while until it gets a go-ahead, if at all. Meanwhile, financial regulators have not been idle. As aforementioned, they have been working on the prospect of so-called CBDCs, with the BIS CBDC working group as the latest initiative in this field [203]. If anything, Libra is proving to be a catalyst for sovereign, public initiatives in the broader payments market.

3.3. Can coins only become credible means of payment if centralised?

An interesting point of view recently floated in legal literature against the backdrop of the first wave of cryptocurrencies, such as Bitcoin, Litecoin and Bitcoin Cash, is that cryptocurrencies can only become credible means of payment if they are centralised[204]. The idea is that there is simply no payment system that is sustainable without a central authority that is able to take responsibility for facilitating payments and can be held accountable and liable towards the community of users if something goes wrong[205]. Accountability must somehow be introduced into the world of cryptocurrencies, but with complete decentralisation this proves to be very difficult. Regulators need a central party to attach regulation to and in a truly decentralised system, such party simply does not exist [206].

The crypto-world is, however, changing. The new generation of cryptocurrencies, and in particular stablecoins, often have a known issuer who plays an important role within the coin's eco-system or require the intervention of third-party accountable institutions, e.g., asset custodians. Payments are still validated in a decentralised way, in the sense that various independently operated nodes play their

---

198 *Ibidem*, 4.

199 See on the difference between permissioned and permissionless systems: R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 15 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

200 D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 9 (electronically available via https://ssrn.com/abstract=3414401). See also LIBRA, "Whitepaper: An introduction to Libra", June 2019, https://libra.org/en-US/white-paper/#introducing-libra, 4.

201 LIBRA, "Whitepaper: An introduction to Libra", June 2019, https://libra.org/en-US/white-paper/#introducing-libra, 4.

202 See 4.1.1 Concern: global stablecoins as a threat to financial stability and monetary policy and 4.1.2 G20 approach: no global private stablecoins before a sufficient regulatory regime is in place, below.

203 See 3.2.1. iv. What's inside the lab?, above.

204 A. ADIMI GIKAY, "Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons From European Union Law", *9 Case Western Reserve Journal of Law, Technology & the Internet 1 (2018)*, March 2018, 29 (electronically available via https://ssrn.com/abstract=3142317).

205 *Ibidem*, 30.

206 A. ADIMI GIKAY, "Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons From European Union Law", *9 Case Western Reserve Journal of Law, Technology & the Internet 1 (2018)*, March 2018, 29 (electronically available via https://ssrn.com/abstract=3142317). See also S. J. HUGHES, "'Gatekeepers' Are Vital Participants in Anti-Money- Laundering Laws and Enforcement Regimes as Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to 'Follow the Money'", *Indiana Legal Studies Research Paper No. 408 (2019)*, August 2019, 20-25 (electronically available via https://ssrn.com/abstract=3436098).

role in the transaction validation process, but contrary to traditional "non-backed" coins there is some level of centralisation, as is for example illustrated by the Libra scheme[207]. Nevertheless, there are still a lot of coins, also new ones, such as algorithmic stablecoins[208], where the link with a liable party cannot be so easily made and it are those coins that currently have the biggest market share in terms of overall market capitalisation. This is problematic from a regulatory point of view, as it hurts the chance of designing an adequate regulatory framework for cryptocurrencies.

[207] See 3.2.2.ii How does Libra work?, above.
[208] See 3.2.2.ii Stablecoin types, above.

4. KEY REGULATORY CONCERNS AND APPROACHES RELATING TO CRYPTO-ASSETS

4.1. Crypto (coins) for payments

4.1.1. Concern: global stablecoins as a threat to financial stability and monetary policy

Global stablecoins may very well provide various benefits to the financial system, most notably by lowering transaction fees in retail cross-border payments[209] and facilitating financial inclusion[210], their global scale also poses new challenges and risks to, amongst others, financial stability and monetary policy[211].

As regards financial stability, various risks can be identified. When a global stablecoin is backed by safe assets, purchases of such assets could cause a shortage of high-quality liquid assets in certain markets, leading to instability[212]. When a global stablecoin is perceived to be a better store of value than a local fiat currency, citizens could collectively run to such a coin in times of financial turmoil, leading to domestic financial instability[213]. Another possible effect of a global stablecoin could be a decline of retail deposits at banks, increasing bank dependence on more costly and volatile sources of funding, again creating potential financial stability risks if banks were to become underfunded[214]. Adding to this, there may also be financial stability risks within global stablecoin schemes themselves. For example, if their credibility gets questioned, many users will want to get out. This could cause serious liquidity problems for banks who would effectively hold the reserve assets that back the coins[215].

If global stablecoins become well established, and the general public starts using them on a day-to-day basis for all payments, substantial control of monetary policy could shift from central banks to private companies[216]. The issue with this is that the latter have no experience with monetary policy, and also have no general obligation towards citizens to act in their best interest[217]. Preliminary research

---

209 See D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 12-13 (electronically available via https://ssrn.com/abstract=3414401); D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 42 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf); V. BRÜL, "Libra – A Differentiated View on Facebook's Virtual Currency Project", *Intereconomics 2020/1 (ZBW – Leibniz Information Centre for Economics)*, 58-59.

210 FSB, "Regulatory issues of stablecoins", October 2019, https://www.fsb.org/wp-content/uploads/P181019.pdf, 2; G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 3; COUNCIL OF THE EUROPEAN UNION, "Joint Statement by the Council and the Commission on Stablecoins", December 2019, 2.

211 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, ii; COUNCIL OF THE EUROPEAN UNION, "Joint Statement by the Council and the Commission on Stablecoins", December 2019, 2; V. BRÜL, "Libra – A Differentiated View on Facebook's Virtual Currency Project", *Intereconomics 2020/1 (ZBW – Leibniz Information Centre for Economics)*, 60.

212 *Ibidem*, 14.

213 D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 23 (electronically available via https://ssrn.com/abstract=3414401); G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 14.

214 FSB, "Regulatory issues of stablecoins", October 2019, https://www.fsb.org/wp-content/uploads/P181019.pdf, 2; G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 13.

215 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 12-13.

216 D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 23 (electronically available via https://ssrn.com/abstract=3414401).

217 *Ibidem*.

on the impact of global stablecoins conducted by the G7 Working Group on Stablecoins suggests that global stablecoins could both [218]:

- weaken the effect of monetary policy on domestic interest rates and credit conditions[219]; and
- increase cross-border capital mobility, which would likely affect so-called capital controls, an important domestic monetary policy measure deployed by certain countries to prevent capital flight in times of severe economic uncertainty[220].

4.1.2. G20 approach: no global private stablecoins before a sufficient regulatory regime is in place

Global stablecoins could have far-reaching consequences for financial stability and monetary policy, if not regulated properly. As crypto-assets, they also pose various other risks that relate to, amongst others, ML/TF, consumer/investor protection and cybersecurity[221]. The G20 Finance Ministers and Central Bank Governors have recently issued a press release indicating that the risks associated with global stablecoin projects need to be further evaluated and appropriately addressed before any global stablecoin project can commence operation[222]. An identical message can be found in a joint statement on stablecoins by the EU Council and the Commission published in December 2019[223].

Moving forward, the EU should align its actions with regard to global stablecoin projects with the ongoing work of international standard-setting bodies like the FSB, who is expected to submit a consultative report on global stablecoins to the G20 Finance Ministers and Central Bank Governors in April 2020, and a final report in July 2020[224]. Indeed, global stablecoins do not only ask for a coordinated approach on an EU level, but for a coordinated global response[225] with a globally consistent set of regulatory standards. They should be established on a sound evidence base and based on general principles. As the EU Council and the Commission rightly indicated in their December 2019 statement on stablecoins, the next step is to gain an even better understanding of all crypto-assets (and not only of (global) stablecoins) and develop an evidence base that could serve as foundation for future EU legislation[226].

4.2. Financial institutions with crypto-assets on their balance sheet

4.2.1. Concern: no credible contribution to own funds

At present, EU financial laws do not prohibit financial institutions, including credit institutions, investment firms, payment institutions and e-money institutions, from holding or gaining exposure to

---

218 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 15.

219 See also V. BRÜL, "Libra – A Differentiated View on Facebook's Virtual Currency Project", *Intereconomics 2020/1 (ZBW – Leibniz Information Centre for Economics)*, 60.

220 D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44*, July 2019, 23 (electronically available via https://ssrn.com/abstract=3414401).

221 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, ii.

222 G20, "Press Release on Global Stablecoins", October 2019, https://www.boj.or.jp/en/announcements/release_2019/data/rel191021e1.pdf, 1.

223 COUNCIL OF THE EUROPEAN UNION, "Joint Statement by the Council and the Commission on Stablecoins", December 2019, 3.

224 FSB, "Regulatory issues of stablecoins", October 2019, https://www.fsb.org/wp-content/uploads/P181019.pdf, 4.

225 COUNCIL OF THE EUROPEAN UNION, "Joint Statement by the Council and the Commission on Stablecoins", December 2019, 3.

226 *Ibidem*.

crypto-assets or from offering services relating to crypto-assets. They are permitted, pursuant to their respective licence status, to carry out:

- regulated financial services listed in, respectively, Annex I to the CRD[227], Annex I to the MiFID II[228], Annex I to the PSD2[229] and Annex I to the EMD2[230]; as well as
- other business activities, provided that they are not prohibited by national law.

Activities involving crypto-assets usually fall within the latter category.

Most crypto-assets either exhibit a high degree of volatility[231] (this is especially the case for traditional "non-backed" cryptocurrencies) or have not yet proven to be truly resilient in times of financial stress (this is the case for most stablecoins in circulation today). In other words, if financial institutions decide to acquire them and take them on their balance sheets or engage in activities that involve them, they could face enormous losses[232]. Moreover, a balance sheet with high-risk crypto-assets on it, could also paint a distorted picture of the financial situation of a financial institution.

As it stands, it seems that there are only a few financial institutions who have acquired crypto-assets and their exposure to such assets remains limited[233], but this, of course, can change and, therefore, supervisory authorities and regulators should remain cautious.

The Basel Committee on Banking Supervision has recently expressed the view that if banks do decide to acquire crypto-assets, or provide related services, they should apply a conservative prudential treatment to such exposures, especially for high-risk crypto-assets[234]. The EBA has previously expressed itself along the same lines in its January 2019 report on crypto-assets[235]. It also observed that clarifications regarding the uncertain accounting treatment of crypto-assets are needed to avoid queries about their prudential treatment under current EU law[236], *i.e.* the CRD/CRR[237].

---

227 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, *OJ L* 176, 27 June 2013, 338 ("CRD").

228 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, *OJ L* 173, 12 June 2014, 349 ("MiFID II").

229 Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *OJ L* 337, 23 December 2015, 35 ("PSD2").

230 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, *OJ L* 267, 10 October 2009, 7 ("EMD2").

231 See also ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 23 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

232 BASEL COMMITTEE ON BANKING SUPERVISION, "Designing a prudential treatment for crypto-assets", December 2019, 11 (electronically available via https://www.bis.org/bcbs/publ/d490.pdf).

233 See EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 23-24. See also BASEL COMMITTEE ON BANKING SUPERVISION, "Designing a prudential treatment for crypto-assets", December 2019, 8 (electronically available via https://www.bis.org/bcbs/publ/d490.pdf).

234 BASEL COMMITTEE ON BANKING SUPERVISION, "Designing a prudential treatment for crypto-assets", December 2019, 1 (electronically available via https://www.bis.org/bcbs/publ/d490.pdf).

235 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 27.

236 *Ibidem*.

237 Regulation (EU) 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, *OJ L* 176, 27 June 2013, 1 ("CRR").

4.2.2. Approach: deduct from own funds

In line with the views expressed by the ECB Crypto-Asset Task Force and the EBA, and as part of a conservative prudential treatment, for now, the best way forward to deal with the uncertainty surrounding crypto-assets, is probably to deduct them from a financial institution's own funds[238]. As it stands, most crypto-assets simply do not constitute a credible contribution to a financial institution's own funds. On the contrary, they qualify as high-risk assets. Therefore, from a prudential perspective, it is recommendable to treat them as such.

Going forward, and as regards banks, the EU would do well to follow up on the work that is currently being done by the Basel Committee on Banking Supervision and the EBA, and assess whether there is a need to further clarify certain rules under the CRD/CRR, given they are not tailored to crypto-assets[239].

4.3. Crypto-assets used for money laundering

4.3.1. Concern: widespread use, but no adequate regime

a. AMLD5 and the 2018 FATF Recommendations

As highlighted in our 2018 study *Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion*[240] and in more recent statements on AML/CFT, like the June 2019 FATF report to the G20 Leaders' Summit[241], cryptocurrencies pose serious money laundering and terrorist financing risks that criminals, money launderers, terrorists and other illicit actors could exploit. The fact that they are fully digital, easily transferable, pseudonymous[242] – and with the use of specific anonymity-enhancing technology even completely anonymous – assets that operate on a decentralised basis, makes them particularly suitable for money laundering and other criminal activities[243].

---

238 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 23-24 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf); EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 27.

239 See also ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 23 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

240 R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, p. 100. (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

241 FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, 2.

242 We reiterate that it is technologically feasible to link cryptocurrency transactions to real-life identities if great effort is made, making cryptocurrencies pseudonymous. However, certain services like mixers and tumblers allow for reduced transparency and increased obfuscation of financial flows, allowing for a high degree of anonymity. See also FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 6 and 36.

243 EUROPEAN COMMISSION, "Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *SWD(2019) 650 final*, July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN, 100; L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them", February 2019, 1 (electronically available via https://ssrn.com/abstract=3328064).

To address the ML/TF risks presented by cryptocurrencies - or, as the EU up until now referred to them, "virtual currencies"[244] - the EU legislator included so-called "*custodian wallet providers*"[245] and "*providers engaged in exchange services between virtual currencies and fiat currencies*" within the scope of the AML/CFT framework by defining them as obliged entities in AMLD5[246]. Member States were supposed to transpose this new EU Directive in their national AML/CFT-legislation by 10 January 2020[247].

As obliged entities, custodian wallet providers and providers engaged in exchange services between virtual currencies and fiat currencies have to comply with the same AML/CFT requirements as banks and other financial institutions[248]. They have to register with national AML authorities, implement customer due diligence controls (so-called "know your customer"-checks), monitor virtual currency transactions, and report suspicious activity to government entities. In addition, only fit and proper persons can be(come) their managers and/or beneficial owners[249].

Since the adoption of AMLD5 on 30 May 2018, the crypto-space has not stood still. New crypto-assets were created, new types of crypto-related services emerged and new service providers entered the crypto-market. In response to these new developments, the FATF adopted changes to its Recommendations – which are considered the global AML/CFT standard – in October 2018, to clarify that they apply to financial activities involving virtual assets, as well as related service providers[250]. It adopted two new Glossary definitions ("virtual asset" – the FATF uses the term "virtual assets" to refer to a very broad category of assets that encompasses what this study has called "crypto-assets" – and "virtual asset service provider"[251]) and it updated Recommendation 15[252]. In its updated form, Recommendation 15 requires countries to regulate virtual asset service providers for AML/CFT purposes, to license or register them[253] and to subject them to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations[254].

---

[244] Virtual currencies are defined in Article 3(18) of 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 June 2015, 73 ("AMLD4"), added by Article 1 of AMLD5. See for the full definition *Table 2: AMLD5 vs. FATF Recommendations*, left column below.

[245] Custodian wallet providers are defined in Article 3(19) of AMLD4, as added by Article 1 of AMLD5. See for the full definition *Table 2: AMLD5 vs. FATF Recommendations*, left column below.

[246] 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 ("AMLD5").

[247] Article 4 AMLD5.

[248] ESAs, "Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector", October 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1, 14.

[249] EUROPEAN COMMISSION, "Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *SWD(2019) 650 final*, July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN, 103.

[250] FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, 2.

[251] See for the full definitions *Table 2: AMLD5 vs. FATF Recommendations*, right column below.

[252] FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 6. See also FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations", June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, 15 and 126-127.

[253] Legal persons have to be licensed or registered in the place of legal creation or incorporation, whereas natural persons have to be licensed or registered in the jurisdiction in which the place of their business is located. See FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 22.

[254] FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, 2; EUROPEAN COMMISSION, "Commission Staff Working Document accompanying the document Report from the Commission to the

In June 2019, the FATF adopted an Interpretative Note to Recommendation 15 (INR 15) to further clarify how the FATF requirements should be applied in relation to virtual assets and virtual asset service providers. INR 15 sets out measures for effective regulation and supervision or monitoring of virtual asset service providers[255]. It requires countries to ensure that their virtual asset service providers assess and mitigate their ML/TF risks and implement customer due diligence controls, record-keeping, suspicious transaction reporting, and screen all transactions for compliance with targeted financial sanctions in line with other entities subject to AML/CFT regulation[256].

The FATF also adopted new Guidance on the application of the risk-based approach to virtual assets and virtual asset service providers in June 2019[257]. The new Guidance expands on its 2015 Guidance for a risk-based approach to virtual currencies, which focused on the points where virtual currency activities intersect with and provide gateways to and from the traditional financial system[258] (*i.e.* so-called virtual currency to fiat currency exchanges[259]). It is intended to help both national authorities to understand and develop regulatory and supervisory responses to virtual asset activities and virtual asset service providers, and private actors seeking to engage in virtual asset activities, to understand their AML/CFT obligations and to effectively comply with them[260].

b. AMLD5 is insufficient

A side-by-side comparison of the latest FATF standards on virtual assets with the AML/CFT-regime for virtual currencies set-out in AMLD5 (see *Table 2: AMLD5 vs. FATF Recommendations* below) shows that the first European AML/CFT-regime for virtual currencies already lags behind of what is considered the current international AML/CFT-standard for crypto-assets (emphasis added in italics).

Table 2: AMLD5 vs. FATF Recommendations

	AMLD5	FATF Recommendations
ASSETS	**Virtual currencies** means 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[261].	A **virtual asset** is a digital representation of value that can be digitally traded, or transferred, *and can be used for payment or investment purposes*. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *SWD(2019) 650 final*, July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN, 97.

255 FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, 2.

256 FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations", June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, 70-71.

257 See FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, p. 57.

258 FATF, "Guidance for a Risk-Based Approach to Virtual Currencies", June 2015, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf, p. 46.

259 See FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 6.

260 FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, 3.

261 Article 3(18) AMLD4.

OBLIGED ENTITIES	**Providers engaged in exchange services between virtual currencies and fiat currencies**. **Custodian wallet provider** means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies[262].	**Virtual asset service provider** means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) exchange between virtual assets and fiat currencies; ii) *exchange between one or more forms of virtual assets*; iii) *transfer of virtual assets*; iv) safekeeping and/or *administration of virtual assets or instruments enabling control over virtual assets*; and v) *participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.*

A first observation is that the AMLD5 definition of "virtual currencies" is a lot narrower than the FATF definition of "virtual assets". It only covers what this study has labelled "cryptocurrencies" and does not encompass other types of crypto-assets, most notably tokens.

A second observation, which we already made in our 2018 study *Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion*[263], is that there are still a number of key crypto-players that fall outside of AMLD5's scope. Various activities of virtual asset services providers, as they are called by the FATF, are not covered by AMLD5 (as highlighted in the right column of *Table 2: AMLD5 vs. FATF Recommendation* above), leaving blind spots in the fight against ML/TF. The following actors covered by the FATF Recommendations are not covered by AMLD5[264]:

- platforms that only offer crypto-to-crypto (*i.e.* virtual to virtual asset) exchange services;
- platforms that facilitate the transfer of crypto-assets as an intermediary; and
- persons that are active in the participation in and provision of financial services related to an issuer's offer and/or sale of crypto-assets.

When AMLD5 was conceived the European legislator did not pay a lot of attention to the existence of these actors and the potential AML/CFT risks they posed. Meanwhile risk awareness has grown. Not only on the European level, within regulatory bodies like the ESMA and the EBA[265], but also on the level

[262] Article 3(19) AMLD4.

[263] R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 76-80 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

[264] EUROPEAN COMMISSION, "Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *SWD(2019) 650 final*, July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN, 103.

[265] ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 36; EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 20-21.

of national Member States[266]. AMLD5 may only just be in full force, from a regulatory perspective, it is already outdated and insufficient to deal with the AML/CFT risks crypto-assets pose today.

4.3.2. Approach: broaden the scope of AMLD5

To bring the European AML/CFT framework up to speed with the current reality in the crypto-space, the EU could consider a number of regulatory actions.

a. Broaden the definition of virtual currencies?

In light of the FATF definition of virtual assets, a first regulatory action to consider is to broaden the scope of the definition of virtual currencies.

i. To include tokens?

The objective of AMLD5 vs. the current definition of virtual currencies

According to Recital 10 of AMLD5: "*Virtual currencies should not to be confused with electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council, with the larger concept of 'funds' as defined in point (25) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council, nor with monetary value stored on instruments exempted as specified in points (k) and (l) of Article 3 of Directive (EU) 2015/2366, nor with in-games currencies, that can be used exclusively within a specific game environment.* ***Although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos. The objective of this Directive is to cover all the potential uses of virtual currencies***" (own emphasis added).

Given this broad objective, one would have expected already in the current status of the law that the definition of virtual currencies would be equally broad. However, this is not the case. On the contrary, the definition of virtual currencies, inserted into the text of AMLD4 as a new Article 3 (18) by Article 1(2)(d) of AMLD5, is at odds with Recital 10. It only covers digital representations of value that are *accepted as a means of exchange*.

This is a lot narrower than the FATF definition of virtual assets cited above, as it does not cover investment and utility tokens[267]. Framed in the taxonomy of crypto-assets set out in *Figure 1: Taxonomy of crypto-assets* above, only cryptocurrencies – but both traditional "non-backed" cryptocurrencies and stablecoins[268] – fall within the scope of the definition of virtual currencies.

---

[266] As highlighted in EUROPEAN COMMISSION, "Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *SWD(2019) 650 final*, July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN, 101-102.

[267] See L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them", February 2019, 13 (electronically available via https://ssrn.com/abstract=3328064). See also 2.5 Tokens can be investment tokens or utility tokens or hybrid forms thereof, above.

[268] Insofar as they do not qualify as e-money schemes. See also L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them", February 2019, 10 (electronically available via https://ssrn.com/abstract=3328064).

Regulators rightly plea for a common AML/CFT approach to all crypto-assets

As the ESMA[269] and the EBA[270] have indicated in their January 2019 reports on crypto-assets (and ICOs), it would make sense to expand the scope of the definition of virtual currencies to all types of crypto-assets and also include (investment and utility) tokens. The reason is simple: tokens make use of the same technology as cryptocurrencies. They can be transferred and stored electronically and, in many cases, traded on the exact same platforms as cryptocurrencies[271]. Their design makes them usable as a "vehicle" to move economic value around, irrespective of their function. In other words, they are equally suitable for ML/TF activities as cryptocurrencies. To create a more adequate AML/CFT regime, the EU should adhere to the latest FATF standards and amend the European AML/CFT framework accordingly, and maybe go even beyond[272].

Cryptocurrencies are still the most widely used crypto-assets for ML/TF, but this could change

Research suggests that traditional "non-backed" cryptocurrencies such as Bitcoin, are still the most widely used crypto-assets for ML/TF[273]. However, given the latest trends in the crypto-space, this could change, if it has not already. The EU would do well to implement an AML/CFT regime that is as technology neutral and as open-ended as possible to account for such change[274], to avoid having to take regulatory action every time an illicit actor changes his particular behaviour.

ii. To include state currencies?

Moving beyond cryptocurrencies and tokens, and more controversial, the EU could also consider broadening the definition of virtual currencies to include state issued digital currencies, or so-called CBDCs, as they could be used to thwart economic sanctions[275]. By including digital state currencies into the scope of the European AML-framework and expanding the list of obliged entities[276], the EU could ensure that questionable foreign actors who try to illegally move their wealth into or through the European financial system using such currencies, are identified, allowing law enforcement agencies to take action against them.

---

269 ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 36.

270 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 20-21. See also ESAs, "Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector", October 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1, 15.

271 L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them", February 2019, 13 (electronically available via https://ssrn.com/abstract=3328064).

272 See 4.3.2.iv and 4.3.2.v, below.

273 For example, according to the Commission Europol still regards Bitcoin as the crypto-asset of choice for the majority of criminals (see EUROPEAN COMMISSION, "Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *SWD(2019) 650 final*, July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN, 101).

274 See also L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them", February 2019, 14 (electronically available via https://ssrn.com/abstract=3328064).

275 *Cf.* CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 29 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/), on Venezuela's plans to start using crypto.

276 See below this page, b.

iii. To include in-game currencies?

Research suggests that in-game currencies, such as "V-Bucks" used in the popular online multiplayer game Fortnite, can also be used to launder money obtained through criminal activities[277]. When in-game currencies have real life value outside of the game and can be transferred from one player to another, criminals can use them to move value around or launder illicit funds through them. For instance, they can buy in-game currencies with illicit funds and then sell them at a discounted rate to other players on the dark web or through social media platforms. While there is currently no hard data available to substantiate this, it is not unlikely that criminals also make use of cryptocurrencies and/or other crypto-assets in this process to even further obfuscate transaction flows[278].

The EU could further study the phenomenon of ML/TF through online games to obtain hard data on the actual scale of misuse and assess, on the basis thereof, whether there is a need to also include in-game currencies in the definition of virtual currencies. Currently, they are excluded because they are not true mediums of exchange[279]. If the conclusion would be that they indeed have to be included in the definition, then it would make sense to update the list of obliged entities accordingly.

b. Broaden the list of obliged entities to all (?) crypto gatekeepers?

Having regard of the FATF definition of virtual asset service providers, a second regulatory action the EU could consider, is to broaden the list of obliged entities. Currently this list includes only two crypto-gatekeepers, namely custodian wallet providers and providers engaged in exchange services between virtual currencies and fiat currencies. A whole variety of crypto players is not yet included. As a result, various activities can still take place outside of the scope of AMLD5. This is problematic because the blind spots can be pursued by criminals, terrorists and other illicit actors to launder money, finance terrorism and/or engage in other illicit activities, such as tax evasion. In view of this, a case can be made for bringing more crypto gatekeepers into the scope of the European AML/CFT framework and for obliging them to implement customer due diligence controls, monitor virtual currency transactions, and report suspicious activity to government entities.

What exactly are the blind spots to be addressed?

i. Crypto-to-crypto exchanges

The first blind spot to be addressed are crypto-to-crypto exchanges. Platforms that only offer exchange services from one crypto-asset to another (for example from a cryptocurrency to a token or from a traditional "non-backed" cryptocurrency to a stablecoin (or vice-versa), or from one traditional "non-backed" cryptocurrency to another, or any other combination of the foregoing) and that do not qualify as custodian wallet providers, remain outside of AMLD5's scope.

Crypto-to-crypto exchanges can add an extra layer of disguise to the origin of crypto-assets (when they later pass through an obliged entity) or even allow crypto-assets to be used completely outside of the monitored system[280]. That is why the FATF has included them in its latest international AML/CFT

---

[277] See A. MOISEIENKO and K. IZENMAN, "Gaming the System: Money Laundering Through Online Games", *RUSI Newsbrief Vol. 39, No. 9*, October 2019, p. 5. (electronically available via https://rusi.org/sites/default/files/20191011_newsbrief_vol39_no9_moiseienko_and_izenman_web.pdf).

[278] *Cf.* FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 18.

[279] Also see Recital 10 of AMLD5 (cited above).

[280] R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 77 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf). *Cf.* See also S. J. HUGHES, "'Gatekeepers' Are Vital Participants in Anti-Money- Laundering Laws and Enforcement Regimes as Permission-less

standards. To remain up to speed and create a more adequate AML/CFT regime, the EU should adhere to these new standards and also include crypto-to-crypto exchanges into the list of obliged entities.

ii. Financial service providers

The second blind spot to be addressed relates to financial service providers who are active in the "*participation in and provision of financial services related to an issuer's offer and/or sale of a crypto-asset*". Natural or legal persons that actively facilitate the offer or issuance of and trading in crypto-assets, whether or not in the context of an ICO, including by accepting purchase orders and funds and purchasing crypto-assets from an issuer to resell and distribute the funds or assets, fall outside of the scope of AMLD5.

As the FATF has rightly pointed out, it makes sense to also bring these actors into the scope of the AML/CFT framework, because they engage in similar activities as financial institutions who participate in the issuance of securities and provide financial services in relation to such issues[281]. Working from the premise of "same risk, same approach", the EU would do well to also add them to the list of obliged entities.

iii. Trading platforms

The third blind spot to be addressed relates to trading platforms. Trading platforms are websites that enable buyers and sellers of crypto-assets to find one another. They function as a market place where different crypto-asset users can post bids and offers. Some trading platforms facilitate trades as an intermediary[282]. However, there are also trading platforms that operate on a decentralised basis: they are not run by an entity that oversees and processes all trades, but they are operated exclusively by software. Neither centrally operated trading platforms, nor their decentralised counterparts are currently obliged entities.

Regulating decentralised trading platforms is very hard, because there is no one to attach regulation to. Regulating centrally operated trading platforms, evidently is more straightforward, as someone fulfils an intermediary function.

The FATF has made two statements on the AML/CFT treatment of trading platforms in its June 2019 Guidance, which can be summarised as follows[283]:

- when a trading platform only provides a forum where buyers and sellers of virtual assets can post their bids and offers, and the parties themselves trade at an outside venue (either through individual wallets or other wallets not hosted by the trading platform), then that trading platform likely falls outside the FATF definition of virtual asset service provider;
- when a trading platform facilitates the exchange and/or transfer of virtual assets, or another financial activity involving virtual assets, including by purchasing virtual assets from a seller (when transactions or bids and offers are matched on the trading platform) and selling them to a buyer, then that trading platform qualifies as a virtual asset service provider conducting exchange and/or transfer activity as a business on behalf of its customers.

Blockchain-Based Transactions Pose Challenges to Current Means to 'Follow the Money'", *Indiana Legal Studies Research Paper No. 408 (2019)*, August 2019, 12 (electronically available via https://ssrn.com/abstract=3436098).

281 See FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 16, fn. 9.

282 *Ibidem*, 15.

283 *Ibidem*, 15.

From these statements it appears that only trading platforms that facilitate the transfer of crypto-assets as an intermediary are covered by the FATF's AML/CFT standards. Pure peer-to-peer trading platforms are not covered, still leaving a blind spot.

When it comes to regulating trading platforms, the EU would do well to at least add those platforms that facilitate the transfer of crypto-assets as an intermediary to the list of obliged entities, adhering to the latest FATF standards[284]. In addition, the ML/TF risks that pure peer-to-peer, decentralised trading platforms pose, should be further assessed and, in view of such risk assessment, adequately addressed.

iv. Issuers or offerors of crypto-assets?

Would it make sense to also include issuers or offerors of crypto-assets into the list of obliged entities? Currently, they fall outside of the scope of the European AML/CFT framework and are also not scrutinised by the FATF.

A compelling argument to include issuers of crypto-assets into the list of obliged entities is that they do not necessarily use financial service providers[285] to structure and conduct the issuance and sale of crypto-assets to prospective users. On the contrary, there are usually no intermediaries involved in the whole process and users buy their crypto-assets, usually tokens or coins that are not mined, directly from the issuer. With that in mind, and having regard of the fact that all crypto-assets possess the same risk for money laundering from a technical perspective[286], the EU could consider bringing issuers of crypto-assets into the scope of the European AML framework. The Commission recently made a similar suggestion during its last supranational risk assessment[287].

v. Other blind spots: non-custodian wallet providers, coin inventors and miners

In our 2018 study *Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion*, we indicated that there are also blind spots in the fight against ML/TF that relate to non-custodian wallet providers, coin inventors and miners. These blind spots have not yet been discussed above. In what follows we briefly reiterate some key points with regard to these players and explain why, at present, they do not require further regulatory action, or require a different approach.

Non-custodian wallet providers

The first blind spot relates to "non-custodian" wallet providers. We reiterate that, broadly speaking, a distinction can be made between three types of wallet providers[288]:

---

[284] *Cf.* France has already done so in its national legislation. See: I. BARSAN, "Regulating the Crypto World – New Developments from France", November 2019, 27 (electronically available via https://ssrn.com/abstract=3484391).

[285] See 2.7 Initial coin offerings: coins or tokens issued by an identifiable issuer, above.

[286] See also L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them", February 2019, 20 (electronically available via https://ssrn.com/abstract=3328064).

[287] See EUROPEAN COMMISSION, "Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *SWD(2019) 650 final*, July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN, 103: "*Once implemented, AMLD5 will improve the situation considerably by making wallet providers and providers of exchange services between virtual currencies and fiat currencies obliged entities, ensuring that they are registered and that only fit and proper persons hold management functions or are beneficial owners. This framework still has to be implemented and* ***it will be necessary to consider extending it to cover*** *other virtual asset service providers, such as* ***initial coin offerors*** *and the providers of exchange services between virtual currencies. The inherent risk exposure is very high due to the characteristics of virtual currencies (internet-based, cross-border and anonymous)*" (own emphasis added).

[288] R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 78 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

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

Only custodian wallet providers, defined in AMLD5 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 crypto-assets themselves.

Non-custodian wallet providers are not scrutinised by the FATF. In its June 2019 Guidance on the application of the risk-based approach to virtual assets and virtual asset service providers the FATF indicated that it does not seek to regulate as virtual asset service providers natural or legal persons that provide ancillary services or products to a virtual asset network, including hardware wallet manufacturers and non-custodial wallets[289]. We see no reason to derogate from this Guidance. Non-custodian wallet providers only provide the technical tools for others to work with and typically do not function as intermediaries, so it does not make much sense to target them for AML/CFT purposes.

Coin inventors

The second blind spot relates to coin inventors, *i.e.* the natural or legal persons who create the technical foundations of a cryptocurrency and set the initial rules for its use. It also does not make much sense to separately target them for AML/CFT purposes, because – just like hardware and software wallet providers – they only provide the technological tools for others to work with[290], unless of course the coin inventor would also be the coin issuer.

Miners

The third and last blind spot relates to cryptocurrency miners. When the text of AMLD5 was drawn up, the Commission saw two main reasons not to include them into the list of obliged entities: 1) they were considered to be more a sort of technical service providers than gatekeepers between the virtual sphere and the real world, and 2) they were thought to be mostly located in China which would make any initiative to target them largely impossible to enforce[291].

The second reason may have had factual grounds when the Commission started studying the mining phenomenon back in 2015-2016, but a lot has changed since then. Data collected by the Cambridge Centre for Alternative Finance in 2018 suggest that mining activity has become more geographically distributed, with China losing relative "market share" to some North American and Scandinavian regions and some Western European countries (e.g., France) also seeing a rising level of activity[292]. If we look at what has happened within the mining community itself, we see that the current mining

[289] See FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 17.

[290] R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 78 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

[291] *Ibidem*, 76.

[292] M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 80 (electronically available via https://ssrn.com/abstract=3306125).

segment is nothing like the mining segment of 2016. First of all, a lot of miners have diversified their activities in terms of the number of coins they mine and are no longer focusing on Bitcoin alone[293]. In addition, new coins have emerged that do not always require big energy-consuming server farms to mine, but that can be mined running a few hardware rigs at home. As it stands, such rigs can be set up by anyone, also by criminal actors[294].

Regulators should be aware that by mining coins, directly or indirectly via front men, criminal actors can get access to clean cash. Newly mined coins are by definition "clean", so if someone (e.g., a bank) is willing to convert them into fiat currency or other crypto-assets, the resulting funds are also clean. This is a reality that is hard to address from a regulatory perspective. A first step could be to try to map the use of this technique and subsequently, if it effectively proves an important blind spot in the fight against money laundering and terrorist financing, to consider appropriate counter measures.

Box 2: On a side note: some thoughts on the environmental impact of cryptocurrencies

Without going into too much detail, it is important to note that not all cryptocurrencies have the same environmental impact. Research published in October 2019 suggests that the electricity consumption for cryptocurrencies that employ a Proof-of-Work (PoW) consensus protocol (e.g. Bitcoin, Monero, …) is considerably higher than for cryptocurrencies following a Proof-of-Stake (PoS) (e.g. Cardano (ADA), …) or hybrid consensus protocol. As a result, many cryptocurrencies have shifted away from the use of pure PoW consensus protocols. However, at the same time, such protocols have also become a lot more efficient; not all coins that employ them today consume as much electricity as Bitcoin.

Cryptocurrencies are commonly perceived to be extremely wasteful. However, according to a benchmarking study presented by the Cambridge Centre for Alternative Finance, most analyses neglect or overlook the energy mix that is used to keep them up and running. It highlights that the environmental impact of cryptocurrencies ultimately depends on the nature of the energy sources used. For example, if miners or transaction validators only rely on fossil fuels for their operations, the environmental impact thereof evidently is a lot bigger than when they resort to a mix of renewables.

That said, the crypto-industry as a whole does have a significant carbon footprint. An interesting question, but one that falls outside the scope of this study, is how regulators should deal with this reality.

c. User registration?

In its 2016 impact assessment, drafted and published in the build-up to AMLD5[295], the Commission put forward a number of options to address the ML/FT risks surrounding virtual currencies. One of the options presented was to target the users (traders, suppliers, customers) of virtual currencies and lift

[293] *Ibidem*, 68-69.

[294] R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 76-77 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

[295] See EUROPEAN COMMISSION, "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*, July 2016, https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52016SC0223, p. 174.

their anonymity. The Commission saw two scenarios to do this: 1) a mandatory registration of users, or 2) a voluntary self-registration of users. Neither of these scenarios were adopted in the end. However, in the final, adopted, text of AMLD5 the Commission did commit itself to draw up a report on the implementation of the Directive by 11 January 2022, and submit it to the European Parliament and the Council. Article 1(44) of AMLD5, which replaces the text of Article 65 of AMLD4 provides that "*the report shall be accompanied, if necessary, by appropriate legislative 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***" (own emphasis added). This seems to point to a system of voluntary self-registration of users.

Meanwhile, during its last supranational risk assessment (published in July 2019), the Commission did not mention user registration at all. This is at least an indication that a system of user registration is not considered a priority and perhaps even that it is no longer on the table. We reiterate that even if a system of voluntary self-registration of users would be put in place, it can very much be doubted that the category that should be targeted the most, users of crypto-assets for illicit purposes, would voluntarily register as a user, as that would be like trusting the thief to come to the police station voluntarily after committing a theft[296].

d. Enhancing the regulatory toolbox and investigative toolbox go hand in hand

The analysis set out above has made clear that the current European legal framework for combatting ML/TF via crypto-assets can be improved, and we invite the EU to do so. However, it should not stop there. Having a regulatory toolbox with high-quality rules is one thing; being able to adequately monitor compliance is another. Enhancing the regulatory and investigative toolbox go hand in hand: to ensure compliance with the regulatory framework, law enforcement agencies at both EU level and Member State level must be able to detect infractions and subsequently sanction them[297]. Therefore, if the EU wants to stay in – and eventually maybe even ahead of – the proverbial game, it should also continue to invest in initiatives that add to the investigative toolbox of law enforcement agencies who are trying to track down ML/TF and other illicit activities such as tax evasion via crypto-assets.

e. A European AML watchdog

Crypto-assets are not tied to national borders, nor are the ML/TF and other illicit activities for which they are sometimes used. If supervisory authorities and law enforcement agencies want to stand a realistic chance in the fight against criminal activities via crypto-assets they need to work together and share information. Unfortunately, this does not always happen. As indicated by the Commission in its last supranational risk-assessment on the European AML/CFT framework[298], cross-border cooperation and coordination between national authorities in the field of AML/CFT still leave much to be desired. To address this problem, on 5 December 2019 the EU Council (ECOFIN) formally invited the Commission "*to explore in particular the possibilities, advantages and disadvantages of conferring certain*

---

[296] R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 80 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

[297] See also R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, p. 100. (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

[298] See EUROPEAN COMMISSION, "Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *COM(2019) 370 final*, July 2019, https://op.europa.eu/en/publication-detail/-/publication/0b2ecb04-aef4-11e9-9d01-01aa75ed71a1/language-en, p. 20.

responsibilities and powers for AML supervision to a Union body with an independent structure and direct powers vis-à-vis certain obliged entities […]"[299].

This study fully endorses this call. The introduction of a European AML watchdog could have various benefits, especially if it is staffed with highly trained IT personnel capable of analysing the AML/CFT risks new technologies bring. It could help promote information-sharing, serve as a new knowledge pool, and provide a more independent approach to AML/CFT cases in comparison to national FIUs.

f. A cashless society with digital money and fully traceable coins (private and/or sovereign) only as a utopia?

As pointed out in Box 1 above, replacing anonymous, untraceable cash with a public, traceable CBDC, or a private equivalent thereof, could theoretically mark the end of many money laundering and other criminal activities. If all payment information[300] is instantly available to law enforcement agencies, or can easily be made available to them, illicit actors will no longer be able to operate in the dark, effectively forcing them to cease many of their operations. However, it is unlikely that citizens will want to fully give up on cash payments any time soon, let alone agree to governments monitoring every payment they make[301]. Politically, the cashless society, a "dream scenario" for supervisory authorities, is most likely a utopia, at least for now.

4.4. Investments in crypto-assets

4.4.1. Concern: unclear regulatory framework

Since the explosion of ICOs in 2017, various regulators have issued statements warning people that investments in crypto-assets are very risky and often fall outside the scope of EU financial services laws (e.g., MiFID II, EMD2, PSD2, MAR[302], the Prospectus Regulation[303], the Transparency Directive[304], etc.) leaving them unprotected if something goes wrong[305]. At the same time, regulators have also pointed out that, depending on their specific design features, certain crypto-assets can be included in the scope of EU financial services laws[306].

---

[299] COUNCIL OF THE EUROPEAN UNION, "Council Conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism", *14823/19*, December 2019, http://data.consilium.europa.eu/doc/document/ST-14823-2019-INIT/en/pdf, 7.

[300] *I.e.* all information on the use of payment instruments and the identity of their holders.

[301] *Cf.* H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 119.

[302] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, *OJ L* 173, 12 June 2014, 1.

[303] Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC, *OJ L* 168, 30 June 2017, 12.

[304] Directive 2013/50/EU of the European Parliament and of the Council of 22 October 2013 amending Directive 2004/109/EC of the European Parliament and of the Council on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market, Directive 2003/71/EC of the European Parliament and of the Council on the prospectus to be published when securities are offered to the public or admitted to trading and Commission Directive 2007/14/EC laying down detailed rules for the implementation of certain provisions of Directive 2004/109/EC, *OJ L* 294, 6 November 2013, 13.

[305] See for example: ESMA, "Statement alerting investors to the high risks of Initial Coin Offerings (ICOs)", November 2017, https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf, p. 2.; AFM, "Warning on Initial Coin Offerings (ICO's): serious risks", https://www.afm.nl/en/professionals/onderwerpen/ico; CMVM, "Warning to investors on Initial Coin Offerings (ICOs)", November 2017, https://www.cmvm.pt/en/Comunicados/Comunicados/Pages/20180119.aspx; FSMA, "Communication on Initial Coin Offerings (ICOs)", *FSMA_2017_20*, November 2017, https://www.fsma.be/sites/default/files/public/content/EN/Circ/fsma_2017_20_en.pdf, p. 4.

[306] See the discussion set out in ESMA, "Annex 1: Legal qualification of crypto-assets – survey to NCAs", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf, p. 28.

In practice, it is not always clear if a crypto-asset effectively falls inside the scope of the existing regulatory framework. This is not only due to the often tailored nature of crypto-assets, but also to the lack of clarity in the financial regulatory framework.

It is accepted that the current perimeter of regulation is such that crypto-assets are, depending on their characteristics, one of the following: financial instruments, electronic money or none of the foregoing (as illustrated in *Figure 4: The ambit of EU financial services laws vis-à-vis crypto-assets* below)[307]. What qualification is most appropriate in a specific case is not always clear, especially when the crypto-asset has a hybrid form with several characteristics. The MiFID II definition of "*financial instruments*"[308], which defines the scope and applicability of most EU financial services laws, and the EMD2 definition of "*electronic money*"[309], were not written with crypto-assets in mind, so in order to find out whether they apply to crypto-asset schemes, they need to be further interpreted. This is especially relevant for the category "*financial instruments*", as it is much more likely that a crypto-asset will qualify as a financial instrument than that it will qualify as electronic money. More in general, although possible, a qualification of crypto-assets as electronic money is in most cases rather unlikely[310]. Crypto-assets as electronic money will, therefore, hereinafter be disregarded.

The need for further interpretation of existing concepts, leads to varying views and opinions. This immediately becomes clear when we look at a survey of 29 National Competent Authorities (NCAs) undertaken by the ESMA in the summer of 2018[311]. When they were asked to indicate whether a sample of six crypto-assets could be legally qualified as MiFID II financial instruments, not all surveyed NCAs provided the same answers.

[307] See *inter alia* EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 15; C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 80; A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", *TBH* 2019/2, (174) 187-191; M. NANNINGS, "Kwalificatie van crypto-assets als effect", *TFR* 2019/12, (623) 625-629; ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 18-21; T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 47-53 (electronically available via https://ssrn.com/abstract=3337514).

[308] "Financial instruments" are defined in Article 4(1)(15) of MiFID II as those "*instruments specified in Section C of Annex I*". These are *inter alia* 'transferable securities', 'money market instruments', 'units in collective investment undertakings' and various derivative instruments.

[309] "Electronic money" is defined in EMD2 in Article 2(2) as "*electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of [PSD2], and which is accepted by a natural or legal person other than the electronic money issuer*".

[310] The EBA has pointed out that, while crypto-assets do not tend to conform to the characteristics of electronic money, there may be cases where, based on the specific characteristics of the crypto-asset in question, the asset will qualify as electronic money and, as a result, fall within the scope of the EMD2. In such cases, authorisation as an electronic money institution is required to carry out activities involving such assets pursuant to Title II of the EMD2, unless a limited network exemption applies in accordance with Article 9 of the EMD2 (see EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 14).

[311] See ESMA, "Annex 1: Legal qualification of crypto-assets – survey to NCAs", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf, p. 28. See also T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 48-49 (electronically available via https://ssrn.com/abstract=3337514).

Figure 4: The ambit of EU financial services laws vis-à-vis crypto-assets

Source: EBA Report on crypto-assets[312].

Moreover, when a crypto-asset is considered to fall inside the regulatory perimeter, it is not always easy to determine how the existing framework should be applied[313].

These circumstances are challenging for all actors involved (including financial supervisors, crypto investment firms and crypto investors) and leads to legal uncertainty. Investors for instance have a hard time figuring out if they enjoy any protection at all. As Steven Maaijoor, chairman of the ESMA, has put it: "*investors may not easily distinguish between those crypto-assets that are financial instruments and those that are not*"[314]. The ESMA has recently stressed that the legal uncertainty surrounding crypto-assets also obstructs the development of a sustainable ecosystem[315]. At present, many legitimate market participants are wondering which rules they should adhere to, if any, to make sure that the activities they conduct are legally compliant.

Along the same lines, there is a risk of regulatory arbitrage. This is illustrated already by the aforementioned potential diverging implementation/supervision of current European definitions in national laws. In addition, an analysis by the EBA and the ESMA suggests that a significant number of crypto-assets and related activities currently fall outside the scope of EU financial services laws[316]. Absent an EU-wide regime, each EU Member State is, in principle, free to establish its own rules as regards these "non-regulated" assets[317]. Since the end of 2018, a limited number of EU Member States has done so, inspired by the idea that "non-regulated" crypto-assets pose similar risks than crypto-assets that are subject to EU financial services laws, in particular in the field of consumer/investor protection[318]. It concerns, for example:

- Malta, where the national legislator has adopted three acts relating to DLT, which entered into force on 1 November 2018: the Virtual Financial Assets Act, the Malta Digital Innovation Authority Act, and the Innovative Technology Arrangement and Services Act[319]. These three acts introduce,

[312] EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 15.

[313] ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 37-29.

[314] S. MAAIJOOR, "Crypto-Assets: time to deliver" (Keynote speech 3rd Annual FinTech Conference), February 2019, https://www.esma.europa.eu/sites/default/files/library/esma71-99-1120_maijoor_keynote_on_crypto-assets_-_time_to_deliver.pdf, 6.

[315] ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 18.

[316] EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 15; ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 20-21.

[317] C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 79.

[318] *Cf.* S. MAAIJOOR, "Crypto-Assets: time to deliver" (Keynote speech 3rd Annual FinTech Conference), February 2019, https://www.esma.europa.eu/sites/default/files/library/esma71-99-1120_maijoor_keynote_on_crypto-assets_-_time_to_deliver.pdf, 6.

[319] I. GAUCI, C. A. GRECH, T. CASSAR and B. SALIBA, "Malta" in M. S. SACKHEIM and N. A. HOWELL (eds.), *The Virtual Currency Regulation Review – Second Edition*, London, Law Business Research, 2019, 201 (electronically available via https://thelawreviews.co.uk//digital_assets/079249ba-c1fd-43cb-b3ad-6c23efb53357/The-Virtual-Currency-Regulation-Review---

among other measures, a requirement for issuers of virtual financial assets to draw up and make available a white paper, licensing requirements for providers of virtual financial services such as brokers, conduct of business rules for license holders and certain AML requirements for license holders[320]; and

- France, where the national legislator has adopted an act on crypto-assets that do not qualify as financial instruments or electronic money, the so-called "*Loi PACTE*" on 22 May 2019. This act introduces, among other measures, an optional visum for ICO issuers regulating primary token emissions, licensing requirements for intermediaries providing digital asset services and certain AML requirements for license holders[321].

These national initiatives are not necessarily aligned with each other, leading to divergent approaches across the EU and regulatory arbitrage between jurisdictions[322]. A crypto-asset that is deemed to be a regulated asset in one jurisdiction may be unregulated in another and investors may face different legal frameworks and different levels of recourse in the event of an issue[323]. This is not only undesirable in view of an EU level playing field, but is also challenging for the overall growth of legitimate crypto-asset schemes[324].

4.4.2. Approach

To adequately address the concerns identified in the current financial regulatory framework regarding crypto-assets, a distinction should be made between crypto-assets that are financial instruments and crypto-assets that are not financial instruments, nor electronic money.

a. Crypto-assets that are financial instruments

As regards crypto-assets that are financial instruments under MiFID II two courses of action can be considered.

The first action relates to the qualification of crypto-assets as financial instruments. As aforementioned, there is currently no common view as to when a crypto-asset qualifies as a MiFID II financial instrument[325]. This is mostly due to the fact that in the course of transposing MiFID II into their national laws EU Member States have defined the term "financial instrument" differently: some have employed

Edition-2.pdf). See also MFSA, "Virtual Financial Assets Framework, Frequently Asked Questions", http://www.mfsa.com.mt/pages/readfile.aspx?f=/files/LegislationRegulation/regulation/VF%20Framework/20180831_VFARFAQs_v1.00.pdf, p. 27.

320 See for a more elaborate analysis of the Maltese regime: C. BUTTIGIEG and C. EFTHYMIOPOULOS, "The regulation of crypto assets in Malta: The Virtual Financial Assets Act and beyond", *Law and Financial Markets Review 2018*, p. 11. (electronically available via https://doi.org/10.1080/17521440.2018.1524687); I. GAUCI, C. A. GRECH, T. CASSAR and B. SALIBA, "Malta" in M. S. SACKHEIM and N. A. HOWELL (eds.), *The Virtual Currency Regulation Review – Second Edition*, London, Law Business Research, 2019, 201-209 (electronically available via https://thelawreviews.co.uk//digital_assets/079249ba-c1fd-43cb-b3ad-6c23efb53357/The-Virtual-Currency-Regulation-Review---Edition-2.pdf).

321 See for a more elaborate analysis of the France regime: I. BARSAN, "Regulating the Crypto World – New Developments from France", November 2019, p. 37. (electronically available via https://ssrn.com/abstract=3484391); H. DE VAUPLANE and V. CHARPIAT, "France" in M. S. SACKHEIM and N. A. HOWELL (eds.), *The Virtual Currency Regulation Review – Second Edition*, London, Law Business Research, 2019, 110-123 (electronically available via https://thelawreviews.co.uk//digital_assets/079249ba-c1fd-43cb-b3ad-6c23efb53357/The-Virtual-Currency-Regulation-Review---Edition-2.pdf).

322 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 15.

323 See also IOSCO, "Consultation Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, 42; IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 44.

324 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 79.

325 See 4.4.1 above.

a restrictive list of examples to define the term transferable securities, others use broader interpretations[326]. To create a level playing field and ensure adequate investor protection across the EU, a common view on the legal qualification of crypto-assets as financial instruments is required. This could take the form of requesting the ESMA to produce further guidance on the interpretation of the list of financial instruments in MiFID II as regards crypto-assets. More intrusive, the EU legislator could implement and enforce a single definition of "transferable securities"[327] and/or amend the list of financial instruments in MiFID II to clarify the application thereof to crypto-assets.

Building on the work of the ESMA and other standard setting bodies like the IOSCO[328], the second action the EU legislator could consider is bringing EU financial services laws up to speed with the unique characteristics of the crypto-sector. As the ESMA has rightly indicated, there are areas that require a re-consideration of specific requirements, or even additional provisions, to allow for an effective application of existing regulations to crypto-assets that are financial instruments[329]. Further research may be required to identify exactly which provisions need an update.

b. Crypto-assets that are not financial instruments, nor electronic money

As regards crypto-assets that do not qualify as MiFID II financial instruments, nor EMD2 electronic money, the EU can either do nothing or implement new rules tailored to the specific risks and issues these crypto-assets pose. Doing nothing leaves investors in the cold, so we agree with the ESMA that the second scenario, where new rules are implemented, is probably the most appropriate course of action[330].

IOSCO research has made clear that "*many of the issues and risks associated with trading crypto-assets* – to be understood here within its broadest meaning and thus encompassing more than investment type assets, or what this study has called investment tokens[331] – *are similar to the issues and risks associated with trading traditional securities or other financial instruments on trading venues*"[332]. It is only appropriate that they are addressed in a similar way. We agree with the ESMA that the EU should, at the very least, put appropriate risk disclosure requirements in place for crypto-assets that do not qualify as financial instruments nor electronic money (including in relation to the issuer, the project, the rights attached to the crypto-asset, the underlying technology used and potential conflicts of interest), so that investors and/or consumers can be made aware of the potential risks prior to committing funds to these crypto-assets[333].

---

[326] ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 39; T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 70 (electronically available via https://ssrn.com/abstract=3337514).

[327] See also T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 70 (electronically available via https://ssrn.com/abstract=3337514).

[328] See IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, p. 51.

[329] ESMA, "Press release Crypto-assets need common EU-wide approach to ensure investor protection", January 2019, https://www.esma.europa.eu/file/49980/download?token=_GEsHR5L, 1; ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 36-39.

[330] ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 41.

[331] Crypto-assets are defined by IOSCO "*a type of private asset that depends primarily on cryptography and DLT or similar technology, as part of its perceived, or inherent value*". See IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 3.

[332] IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 6.

[333] ESMA, "Press release Crypto-assets need common EU-wide approach to ensure investor protection", January 2019, https://www.esma.europa.eu/file/49980/download?token=_GEsHR5L, 1; ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 40. The ESMA rightly

The question is whether this is enough to solve the issue of regulatory arbitrage between EU Member States and to ensure appropriate standards for consumer/investor protection. Should the EU not do more and adopt a wider "bespoke" regime for non-financial instrument/non-e-money crypto-assets and related activities, and for example introduce licensing requirements for brokers, asset managers and other intermediaries? When considering this, as the ESMA has rightly pointed out, the EU should be mindful of the trade-offs a wider regulation of crypto-assets could have, such as risking legitimising them and encouraging wider adoption[334]. That is why the ESMA advises, at this stage, to focus the regime for crypto-assets that are not financial instruments, nor electronic money, on warning buyers about the risks of those crypto-assets, instead of a more elaborate regime[335].

Many non-financial instrument/non-e-money crypto-assets pose risks and issues that are similar to traditional financial instruments or electronic money. However, the EU should note that depending on their design and whether they are tradeable on secondary markets, it may also be possible that they have little to no relation with financial markets. For example, when a utility token is non-tradable (such token is usually referred to as a "pure" utility token[336]), it can only be redeemed for certain goods or services, similar to a non-tradeable voucher. Such instrument probably requires a different treatment.

More in general, we agree with the ESMA that if the EU legislator were to consider adopting further regulation, the proposed regime must be flexible enough to capture the wide variety of characteristics and risk factors that non-financial instrument/non-e-money crypto-assets introduce[337]. Moreover, it should be as technology neutral as possible, to make it as future-proof as practically possible[338].

4.5. Cybersecurity issues

4.5.1. Concern: safeguarding users' crypto-assets and rebutting ransomware attacks

a. Safeguarding users' crypto-assets

More and more crypto-asset users are storing the private keys to access their crypto-asset funds at online storage providers or crypto-exchanges who offer custody services to their customers in order to make their overall experience in the crypto-world more user-friendly[339]. This practice is not without its

highlights that: "*To date, the quality, transparency and disclosure of risks in so-called ICO 'white papers' varies greatly and often emphasises likelihood of financial returns to encourage speculative 'investment' behaviour by consumers, even where a crypto-asset lacks the legal characteristics to be a financial instrument*".

334 ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 40.

335 *Ibidem*, 40-41.

336 A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", *TBH* 2019/2, (174) 184-185.

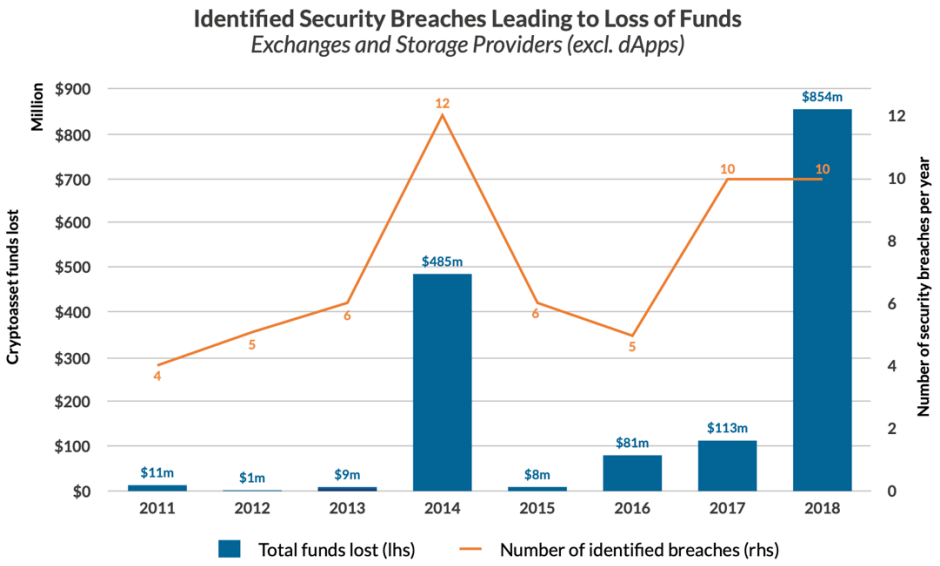
337 ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 41.

338 See also EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 19.

339 M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 63 (electronically available via https://ssrn.com/abstract=3306125). See also IOSCO, "Consultation Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, 12-13; IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 12-13. See on the use of "keys" also R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 16-17 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

risks. If a user's private keys are stolen or made inaccessible[340] during a hack of the storage provider or exchange, he can no longer access his crypto-assets, resulting in a loss of funds[341]. Unfortunately, cyber incidents at exchanges are on the rise[342]. Over the past few years, users of crypto-assets have lost several hundreds of millions of US Dollars worth of crypto-asset funds as a result of security breaches at exchanges and storage providers (see *Figure 5: Loss of crypto-assets* below). In 2019, thefts were reported to even exceed a value of more than $1 billion[343].

Figure 5: Loss of crypto-assets



Source: 2nd Global Cryptoasset benchmarking study – Cambridge Centre for Alternative Finance[344].

Cybersecurity has become a major issue in the field of crypto-assets, as has the effective safeguarding of users' crypto-assets. Stolen crypto-assets typically find their way to illegal markets and are used to fund further criminal activity. For example, recent research by UN experts has revealed that cyber actors employed by the Democratic People's Republic of Korea have stolen an estimated $2 billion in fiat currencies and cryptocurrencies from banks and crypto-exchanges to fund the production of weapons of mass destruction[345].

---

340 IOSCO, "Consultation Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, 13; IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 13.

341 *Ibidem*.

342 See M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 63 (electronically available via https://ssrn.com/abstract=3306125); G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 8.

343 CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 17 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/).

344 M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 63 (electronically available via https://ssrn.com/abstract=3306125).

345 M. NICHOLS, "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report", August 2019, https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX; CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 30 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/).

b. Rebutting ransomware attacks

An additional concern for regulators relates to so-called ransomware attacks. Research indicates that criminals who are involved in such ransomware attacks, whereby the access to computers and networks is locked until the victim pays a certain ransom, often ask victims to pay the ransom in (traditional "non-backed") cryptocurrencies such as Bitcoin[346]. Cryptocurrencies allow criminals to monetise on ransomware attacks without revealing their real-life identities, making such attacks very interesting and lucrative exploits.

Absent regulatory or other actions, the number of ransomware attacks involving crypto-ransoms is not likely to decrease any time soon.

4.5.2. Approach: risk management policies, independent systems audits and coin blacklisting (?)

a. Risk management policies and independent systems audits

A present, the crypto-community is already taking action to address cybersecurity concerns itself. For example, crypto-exchanges and storage providers have been employing IT security specialists and organising basic cybersecurity training programmes for their staff on a regular basis[347]. In addition, they have also been conducting internal security audits quite frequently[348]. However, external audits by independent experts appear a lot less frequent, if they are conducted at all[349].

In the current state of the EU regulatory framework, there are no specific laws that set-out minimum standards for cybersecurity to be complied with by intermediaries who offer custodial services for crypto-assets, *i.e.* exchanges and storage providers. In line with remarks made by the IOSCO[350], the EU should consider introducing such standards for intermediaries operating within the EU. It could, for example, introduce an obligation for each intermediary offering custodial services to EU citizens to (i) draw up and implement an IT risk management policy adhering to certain IT security standards, and (ii) appoint an independent IT expert to conduct an external security audit on a regular basis.

b. Coin blacklisting (?)

To decrease the number of successful ransomware attacks involving crypto-ransoms, overall cyber-security awareness can be improved. In addition, a regulatory response could be to make it harder for criminals to use the crypto-ransoms they have collected for other, future, transactions. This could be done by blacklisting the coins used to pay a crypto-ransom[351]. The coins would get a "tag" so to speak,

---

[346] CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 20-21 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/); S. J. HUGHES, "'Gatekeepers' Are Vital Participants in Anti-Money- Laundering Laws and Enforcement Regimes as Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to 'Follow the Money'", *Indiana Legal Studies Research Paper No. 408 (2019)*, August 2019, 38 (electronically available via https://ssrn.com/abstract=3436098); X. LI and A. B. WHINSTON, "Analyzing Cryptocurrencies", October 2019, 1 and 4 (electronically available via https://ssrn.com/abstract=3500276); M. MÖSER and A. NARAYANAN, "Effective Cryptocurrency Regulation Through Blacklisting", October 2019, 1 (electronically available via https://maltemoeser.de/paper/blacklisting-regulation.pdf).

[347] M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 64 (electronically available via https://ssrn.com/abstract=3306125).

[348] *Ibidem*, 66.

[349] *Ibidem*, 65.

[350] See IOSCO, "Consultation Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, 22-24; IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 22-24.

[351] See on the concept of blacklisting: M. MÖSER and A. NARAYANAN, "Effective Cryptocurrency Regulation Through Blacklisting", October 2019, p. 24. (electronically available via https://maltemoeser.de/paper/blacklisting-regulation.pdf).

much like physical banknotes would get marked, which would make it more difficult for criminals to move them through legitimate channels or effectively spend them, making the collection of a crypto-ransom less interesting. The idea is that legitimate market participants will not want to get associated with tainted coins. The EU should follow-up on the technical feasibility of coin blacklisting – which could have a much broader application than only rebutting ransomware attacks[352] – and the potential effects it could have on the crypto-market as a whole.

[352] It could for example also be used in the fight against ML/TF. See: M. MÖSER and A. NARAYANAN, "Effective Cryptocurrency Regulation Through Blacklisting", October 2019, 1-4 (electronically available via https://maltemoeser.de/paper/blacklisting-regulation.pdf).

5. SUBSIDIARITY: RULEMAKING AT THE MOST INTERNATIONAL LEVEL TO AVOID REGULATORY ARBITRAGE, ESPECIALLY GIVEN CROSS-BORDER NATURE

Crypto-assets are a global phenomenon: they are created by private actors in various countries all over the world, they are cross-border in their application and infrastructure, and they are easily accessible, transferable, exchangeable and tradeable from nearly anywhere in the world. As a result, they do not only present regulatory challenges within EU borders, but far beyond. To address these challenges, regulatory authorities will have to step in. In some countries legislators have already taken action (examples in the field of investor protection include Switzerland, Malta and France) or are planning to do so. These national initiatives are not necessarily aligned with each other, leading to regulatory arbitrage. To avoid regulatory arbitrage, rulemaking on crypto-assets should take place at the European level, preferably in the execution of international standards.

To further illustrate why international standard setting is key, we hereinafter take AML/CFT rules as a leading example.

Just like crypto-assets, money laundering and terrorist financing are global phenomena that do not stop at EU borders[353]. Criminals and terrorists tend to look for loopholes or gaps in the regulatory framework when developing their ML/TF activities. So, if a country or a region has AML rules that are more favourable towards them, in the sense that they leave more leeway for their illicit activities, then they are likely to set up shop in these countries or regions and use them as a gateway to launder their money. This undoubtedly also holds true for ML/TF activities involving crypto-assets[354]. If for example the US would uphold stronger AML/CFT rules *vis-à-vis* crypto-assets than the EU (or even individual EU countries), ML/TF activities via crypto-assets are likely to shift to the EU territory. However, if the same AML/CFT standards are upheld in both regions, then the chances of effectively rooting out such activities are a lot bigger. It thus makes sense to set AML/CFT standards, at the international level. As an intergovernmental "policy-making body", the FATF is doing precisely that.

The EU and the EU Member States should continue to contribute to the work of the FATF and the international standards set by the FATF should continue to be incorporated into EU law in a timely and comprehensive manner to ensure full compliance throughout the internal market and the international financial system[355].

In this respect, the EU could do better. As illustrated above, the latest EU AML/CFT rules for virtual currencies, set out in AMLD5, were already outdated well before EU Member States were supposed to transpose them into their national AML/CFT laws, *i.e.* on 10 January 2020[356]. The EU is clearly lagging behind on international AML/CFT standards and has regulatory work to do. If the EU would remain inactive, individual Member States can already take the lead – and perhaps even should, given the risk-based approach of AMLD and their individual memberships of the FATF – and amend their domestic AML legislation to comply with the latest FATF Recommendations, or even go beyond[357]. It is, however, clear that such domestic actions alone are not sufficient, as they only offer legal certainty within one

[353] See also COUNCIL OF THE EUROPEAN UNION, "Council Conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism", *14823/19*, December 2019, http://data.consilium.europa.eu/doc/document/ST-14823-2019-INIT/en/pdf, 4.

[354] See also C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 79.

[355] *Ibidem*, 5.

[356] See 4.3.1 b AMLD5 is insufficient, above.

[357] See 4.3.2.iv and 4.3.2.v, above.

country's borders. To avoid an unlevel playing field and legal uncertainty in a cross-border context, regulatory action at a higher level is required.

REFERENCES

- ADIMI GIKAY, A., "Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons From European Union Law", *9 Case Western Reserve Journal of Law, Technology & the Internet 1 (2018)*, March 2018, p. 35. (electronically available via https://ssrn.com/abstract=3142317).
- AFM, "Warning on Initial Coin Offerings (ICO's): serious risks", https://www.afm.nl/en/professionals/onderwerpen/ico.
- AMSDEN, Z., ARORA, R., BANO, S., BAUDET, M., BLACKSHEAR, S., BOTHRA, A., CABRERA, G., CATALINI, C., CHALKIAS, K., CHENG, E., CHING, A., CHURSIN, A., DANEZIS, G., DI GIACOMO, G., DILL, D. L., DING, H., DOUDCHENKO, N., GAO, V., GAO, Z., GARILLOT, F., GORVEN, M., HAYES, P., HOU, J. M., HU, Y., HURLEY, K., LEWI, K., LI, C., LI, Z., MALKHI, D., MARGULIS, S., MAURER, B., MOHASSEL, P., DE NAUROIS, L., NIKOLAENKO, V., NOWACKI, T., ORLOV, O., PERELMAN, D., POTT, A., PROCTOR, B., QADEER, S., RAIN, RUSSI, D., SCHWAB, B., SEZER, S., SONNINO, A., VENTER, H., WEI, L., WERNERFELT, N., WILLIAMS, B., WU, Q. , YAN, X., ZAKIAN, T. and ZHOU, R., "The Libra Blockchain", September 2019, https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf, p. 29.
- ANCHUSTEGUI, I. H. and HUNTER, T. S., "Oil as Currency: Venezuela's Petro, a New 'Oil Pattern'?", November 2018, p. 20. (electronically available via https://ssrn.com/abstract=3291272).
- ANNUNZIATA, F., "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", *Bocconi Legal Studies Research Paper No. 2636561*, February 2019, p. 50. (electronically available via https://ssrn.com/abstract=3332485).
- BAIN, B. and WEINSTEIN, A., "Facebook Says Libra Won't Launch Until Regulators Satisfied", July 2019, https://www.bloomberg.com/news/articles/2019-07-15/facebook-says-libra-won-t-launch-until-regulators-satisfied.
- BARONTINI, C. and HOLDEN, H., "Proceeding with caution – a survey on central bank digital currency" (BIS Papers No 101), January 2019, https://www.bis.org/publ/bppdf/bispap101.pdf, p. 20.
- BARSAN, I., "Regulating the Crypto World – New Developments from France", November 2019, p. 37. (electronically available via https://ssrn.com/abstract=3484391).
- BASEL COMMITTEE ON BANKING SUPERVISION, "Designing a prudential treatment for crypto-assets", December 2019, p. 18. (electronically available via https://www.bis.org/bcbs/publ/d490.pdf).
- BINDSEIL, U., "Central bank digital currency - financial system implications and control", July 2019, p. 39. (electronically available via https://ssrn.com/abstract=3385283).
- BIS, "Central bank group to assess potential cases for central bank digital currencies", 21 January 2019, https://www.bis.org/press/p200121.htm.
- BLEMUS, S. and GUEGAN, D., "Initial Crypto-Asset Offerings (ICOs), Tokenization and Corporate Governance", January 2019, p. 31. (electronically available via https://ssrn.com/abstract=3350771).
- BROWN, C., DOLAN, T. and BUTLER, K., "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, 74-101.
- BRÜL, V., "Libra – A Differentiated View on Facebook's Virtual Currency Project", *Intereconomics 2020/1 (ZBW – Leibniz Information Centre for Economics)*, 54-61.

- BULLMANN, D., KLEMM, J. and PINNA, A., "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, p. 55. (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).
- BURILOV, V., "Utility Token Offerings and Crypto Exchange Listings: how regulation can help?", November 2018, p. 74. (electronically available via https://ssrn.com/abstract=3284049).
- BUTTIGIEG, C. and EFTHYMIOPOULOS, C., "The regulation of crypto assets in Malta: The Virtual Financial Assets Act and beyond", Law and Financial Markets Review 2018, p. 11. (electronically available via https://doi.org/10.1080/17521440.2018.1524687).
- CALCATERRA, C., KAAL, W. A. and RAO, V., "Stable cryptocurrencies – First Order Principles", *Stanford Journal of Blockchain Law & Policy (2019)*, June 2019, p. 30. (electronically available via https://ssrn.com/abstract=3402701).
- CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, p. 37. (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/).
- CMVM, "Warning to investors on Initial Coin Offerings (ICOs)", November 2017, https://www.cmvm.pt/en/Comunicados/Comunicados/Pages/20180119.aspx.
- CONGRESSIONAL RESEARCH SERVICE, "Digital Assets and SEC Regulation", January 2020, p. 16. (electronically available via https://www.hsdl.org/?view&did=833720).
- COUNCIL OF THE EUROPEAN UNION, "Council Conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism", *14823/19*, December 2019, http://data.consilium.europa.eu/doc/document/ST-14823-2019-INIT/en/pdf, p. 7.
- COUNCIL OF THE EUROPEAN UNION, "Joint Statement by the Council and the Commission on Stablecoins", December 2019, p. 3.
- CPMI, "Central bank digital currencies", March 2018, p. 34. (electronically available via https://www.bis.org/cpmi/publ/d174.pdf).
- DE VAUPLANE, H. and CHARPIAT, V., "France" in M. S. SACKHEIM and N. A. HOWELL (eds.), The Virtual Currency Regulation Review – Second Edition, London, Law Business Research, 2019, 110-123 (electronically available via https://thelawreviews.co.uk//digital_assets/079249ba-c1fd-43cb-b3ad-6c23efb53357/The-Virtual-Currency-Regulation-Review---Edition-2.pdf).
- DE VAUPLANE, H., "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, 102-121.
- EBA and ESMA, "Joint EBA ESMA response to the letter of 19 July 2019 on crypto-assets", August 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-164-2554_joint_eba_esma_reply_to_vp_dombrovskis_re_crypto-assets.pdf, p. 2.
- EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, p. 30.
- ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223,* May 2019, p. 38. (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).

- ECB, "Exploring anonymity in central bank digital currencies", In Focus Issue No 4, December 2019, p. 11. (electronically available via https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf).
- ELLSWORTH, B., "Special Report: In Venezuela, new cryptocurrency is nowhere to be found", August 2018, https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U?utm_source=MIT+Technology+Review&utm_campaign=e648089a9e-EMAIL_CAMPAIGN_2018_02_27_COPY_02&utm_medium=email&utm_term=0_997ed6f472-e648089a9e-157724665.
- ENGERT, W. and FUNG, B. S. C., "Central Bank Digital Currency: Motivations and Implications", *Bank of Canada Staff Discussion Paper*, November 2017, p. 30. (electronically available via https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf).
- ESAs, "Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector", October 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1, p. 84.
- ESMA, "Advice on Initial Coins Offerings and Crypto-Assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, p. 49.
- ESMA, "Annex 1: Legal qualification of crypto-assets – survey to NCAs", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf, p. 28.
- ESMA, "Press release Crypto-assets need common EU-wide approach to ensure investor protection", January 2019, https://www.esma.europa.eu/file/49980/download?token=_GEsHR5L, p. 3.
- ESMA, "Statement alerting investors to the high risks of Initial Coin Offerings (ICOs)", November 2017, https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf, p. 2.
- EUROPEAN COMMISSION, "Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *SWD(2019) 650 final*, July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN, p. 270.
- EUROPEAN COMMISSION, "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*, July 2016, https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52016SC0223, p. 174.
- EUROPEAN COMMISSION, "Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", *COM(2019) 370 final*, July 2019,

https://op.europa.eu/en/publication-detail/-/publication/0b2ecb04-aef4-11e9-9d01-01aa75ed71a1/language-en, p. 20.

- EY, "Research: initial coin offerings (ICOs)", December 2017, p. 44. (electronically available via http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf).
- FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, p. 6.
- FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, p. 57.
- FATF, "Guidance for a Risk-Based Approach to Virtual Currencies", June 2015, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf, p. 46.
- FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations", June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, p. 132.
- 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. 11.
- FISH, C., "Initial coin offerings (ICOs) to finance new ventures", *Journal of Business Venturing, 34(1)*, January 2019, p. 48. (electronically available via https://ssrn.com/abstract=3147521).
- FLOYD, D., "Venezuela's Petro Isn't Oil-Backed. It's Not Even a Cryptocurrency (Opinion)", June 2019, https://www.investopedia.com/news/venezuela-petro-not-cryptocurrency/.
- FOLEY, S., KARLSEN, J. R. and J. PUTNIŅŠ, T., "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, p. 63. (electronically available via https://ssrn.com/abstract=3102645).
- FSB, "Crypto-assets: work underway, regulatory approaches and potential gaps", May 2019, https://www.fsb.org/wp-content/uploads/P310519.pdf, p. 11.
- FSB, "Regulatory issues of stablecoins", October 2019, https://www.fsb.org/wp-content/uploads/P181019.pdf, p. 4.
- FSMA, "Communication on Initial Coin Offerings (ICOs)", FSMA_2017_20, November 2017, https://www.fsma.be/sites/default/files/public/content/EN/Circ/fsma_2017_20_en.pdf, p. 4.
- G20, "Press Release on Global Stablecoins", October 2019, https://www.boj.or.jp/en/announcements/release_2019/data/rel191021e1.pdf, p. 1.
- G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, p. 31.
- GAUCI, I., GRECH, C. A., CASSAR, T. and SALIBA, B., "Malta" in M. S. SACKHEIM and N. A. HOWELL (eds.), *The Virtual Currency Regulation Review – Second Edition*, London, Law Business Research, 2019, 201-209 (electronically available via https://thelawreviews.co.uk//digital_assets/079249ba-c1fd-43cb-b3ad-6c23efb53357/The-Virtual-Currency-Regulation-Review---Edition-2.pdf).

- GREENBERG, A., "Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire", https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.
- HACKER, P., and THOMALE, C., "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", November 2017, p. 45. (electronically available via https://ssrn.com/abstract=3075820).
- HAFFKE, L., FROMBERGE, M. and ZIMMERMANN, P., "Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them", February 2019, p. 23. (electronically available via https://ssrn.com/abstract=3328064).
- HOUBEN, R. and SNYERS, A., "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", *European Parliament study*, July 2018, p. 100. (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).
- HUGHES, S. J., "'Gatekeepers' Are Vital Participants in Anti-Money- Laundering Laws and Enforcement Regimes as Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to 'Follow the Money'", *Indiana Legal Studies Research Paper No. 408 (2019)*, August 2019, p. 40. (electronically available via https://ssrn.com/abstract=3436098).
- Introductory statement by Christine Lagarde, President of the ECB, at the ECON committee of the European Parliament, 2 December 2019, https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp191202~f8d16c9361.en.html.
- IOSCO, "Consultation Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, p. 42.
- IOSCO, "Final Report on the Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, p. 51.
- IOSCO, "Statement on IOSCO study of emerging global stablecoin proposals", November 2019, https://www.iosco.org/news/pdf/IOSCONEWS550.pdf, p. 2.
- JIA, C., "China's digital currency may be world first", 9 September 2019, https://www.telegraph.co.uk/china-watch/technology/china-digital-currency/.
- LE MOIGN, C., "ICO françaises: un nouveau mode de financement?", November 2018, p. 26. (electronically available via https://www.amf-france.org/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives?docId=workspace%3A%2F%2FSpacesStore%2F27604d2f-6f2b-4877-98d4-6b1cf0a1914b).
- LI, X. and WHINSTON, A. B., "Analyzing Cryptocurrencies", October 2019, p. 11. (electronically available via https://ssrn.com/abstract=3500276).
- LIBRA, "Whitepaper: An introduction to Libra", June 2019, https://libra.org/en-US/white-paper/#introducing-libra, p. 12.
- MAAIJOOR, S., "Crypto-Assets: time to deliver" (Keynote speech 3rd Annual FinTech Conference), February 2019, https://www.esma.europa.eu/sites/default/files/library/esma71-99-1120_maijoor_keynote_on_crypto-assets_-_time_to_deliver.pdf, p. 7.

- MAAS, T., "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, p. 77. (electronically available via https://ssrn.com/abstract=3337514).
- MFSA, "Virtual Financial Assets Framework, Frequently Asked Questions", http://www.mfsa.com.mt/pages/readfile.aspx?f=/files/LegislationRegulation/regulation/VF%20Framework/20180831_VFARFAQs_v1.00.pdf, p. 27.
- MOISEIENKO, A. and IZENMAN, K., "Gaming the System: Money Laundering Through Online Games", *RUSI Newsbrief Vol. 39, No. 9*, October 2019, p. 5. (electronically available via https://rusi.org/sites/default/files/20191011_newsbrief_vol39_no9_moiseienko_and_izenman_web.pdf).
- MOMTAZ, P., "Initial Coin Offerings" July 2018, p. 49. (electronically available via https://ssrn.com/abstract=3166709).
- MÖSER, M. and NARAYANAN, A., "Effective Cryptocurrency Regulation Through Blacklisting", October 2019, p. 24. (electronically available via https://maltemoeser.de/paper/blacklisting-regulation.pdf).
- NANNINGS, M., "Kwalificatie van crypto-assets als effect", *TFR* 2019/12, 623-632.
- NICHOLS, M., "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report", August 2019, https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX.
- OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, p. 36. (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).
- PERLMAN, L., "A Model Crypto-Asset Regulatory Framework", May 2019, p. 9. (electronically available via https://ssrn.com/abstract=3370679).
- PERNICE, I. G.A., HENNINGSEN, S., PROSKALOVICH, R., FLORIAN, M., ELENDNER, H. and SCHEUERMANN, B., "Monetary Stabilization in Cryptocurrencies—Design Approaches and Open Questions", June 2019, p. 13. (electronically available via https://ssrn.com/abstract=3398372).
- RAUCHS, M., BLANDIN, A., KLEIN, K., PIETERS, G., RECANATINI, M. and ZHANG, B., "2nd Global Cryptoasset Benchmarking Study", December 2018, p. 96. (electronically available via https://ssrn.com/abstract=3306125).
- ROHR, J. and WRIGHT, A., "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets", *Cardozo Legal Studies Research Paper No. 527*, October 2017, p. 115. (electronically available via https://ssrn.com/abstract=3048104).
- SAPKOTA, N. and GROBYS, K., "Blockchain Consensus Protocols, Energy Consumption and Cryptocurrency Prices", October 2019, p. 29. (electronically available via https://ssrn.com/abstract=3403983).
- SECURITIES AND MARKETS STAKEHOLDER GROUP, "Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets", *ESMA22-106-1338*, October 2018, p. 36. (electronically available via https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf).
- SNYERS, A. and PAUWELS, K., "De ITO: a new kid on the block in het kapitaalmarktenrecht", *TBH* 2019/2, 174-206.

- SNYERS, A. and PAUWELS, K., "ICOs in Belgium: down the rabbit hole into legal no man's land? Part 1", *ICCLR* 2018, Vol. 29, Issue 8, 483-510.
- VILLEROY DE GALHAU, F., "Speech on Central bank digital currency and innovative payments", December 2019, p. 7. (electronically available via https://www.banque-france.fr/sites/default/files/medias/documents/2019.12.04_conference_acpr_en_v5.pdf).
- ZETZSCHE, D. A., BUCKLEY, R. P. and ARNER, D. W., "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", *European Banking Institute Working Paper Series 2019/44,* July 2019, p. 30. (electronically available via https://ssrn.com/abstract=3414401).
- ZETZSCHE, D. A., 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", *University of Luxembourg Law Working Paper No. 11/2017*, July 2018, p. 43. (electronically available via https://ssrn.com/abstract=3072298).
- https://blog.bankera.com/2018/05/07/why-is-the-bnk-token-unique/.
- https://coinmarketcap.com.
- https://crypterium.com.
- https://filecoin.io.
- https://gemini.com/dollar.
- https://golem.network.
- https://makerdao.com/en/.
- https://tether.to.
- https://www.paxos.com/pax/.
- https://www.reuters.com/article/sweden-cenbank/swedens-central-bank-says-to-launch-digital-currency-pilot-project-idUSL8N28N463.
- https://www.reuters.com/article/us-eu-cryptocurrency-regulations/alarmed-by-libra-eu-to-look-into-issuing-public-digital-currency-draft-idUSKBN1XF1VC.
- https://www.riksbank.se/en-gb/payments--cash/e-krona/.

This study, prepared by Policy Department A, sets out recent developments regarding crypto-assets. These relate mainly to the continuing use of crypto-assets for money laundering and terrorist financing, the massive growth of private ''tokens'' used to raise funds, and to the emergence of stablecoins and central bank digital currencies. The study, furthermore, addresses key regulatory concerns, taking into account these recent developments, and suggests regulatory responses.

PE 648.779
IP/A/ECON/2019-33

Print ISBN 978-92-846-6503-7 | doi:10.2861/895050 | QA-03-20-236-EN-C
PDF ISBN 978-92-846-6502-0 | doi:10.2861/25063 | QA-03-20-236-EN-N