



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Εθνικόν και Καποδιστριακόν  
Πανεπιστήμιον Αθηνών

— ΙΔΡΥΘΕΝ ΤΟ 1837 —

## ΝΟΜΙΚΗ ΣΧΟΛΗ

Π.Μ.Σ.: ΔΗΜΟΣΙΟ ΔΙΚΑΙΟ

ΕΙΔΙΚΕΥΣΗ: ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΟ ΔΙΚΑΙΟ (Financial Regulation)

ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΕΤΟΣ: 2019 - 2020

### ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της **Μαρίας Πετράκη του Σάββα**

A.M.: 7340012519013

**“Cryptocurrencies as investment products: Financial risks and regulatory approaches”**

#### Επιβλέποντες καθηγητές:

- α) Καθηγητής, κ. Χρήστος Γκόρτσος
- β) Επίκουρος Καθηγητής, κ. Ανδρέας Τσουρουφλής
- γ) Επίκουρος Καθηγητής, κ. Νικόλαος Παπασπύρου

Αθήνα, Νοέμβριος 2020

Copyright © Μαρία Σ. Πετράκη 2020

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα.

Οι απόψεις και θέσεις που περιέχονται σε αυτήν την εργασία εκφράζουν την συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

*...στην Πηνελόπη και στον Γιάνη*

## Περίληψη

Την τελευταία δεκαετία και με έναυσμα την δημιουργία του Bitcoin, του πρώτου βασισμένου στην κρυπτογράφηση και την τεχνολογία blockchain νομίσματος, χιλιάδες κρυπτονομίσματα (cryptocurrencies) έκαναν την εμφάνισή τους, δημιουργώντας μία δυναμική και συνεχώς αναπτυσσόμενη επενδυτική αγορά. Στην παρούσα μελέτη, τα ιδιότυπα αυτά ψηφιακά περιουσιακά στοιχεία προσεγγίζονται όχι ως μέσα πληρωμής αλλά ως επενδυτικά προϊόντα, βάσει των τελευταίων οικονομικών και νομικών εξελίξεων σε Ευρωπαϊκό και παγκόσμιο επίπεδο.

Η μελέτη διαρθρώνεται σε τρία μέρη. Στο πρώτο κεφάλαιο, επιχειρείται μία διάκριση ανάμεσα στους βασικούς τύπους κρυπτονομισμάτων και παρουσιάζονται τα επενδυτικά τους χαρακτηριστικά. Στη συνέχεια, στο δεύτερο κεφάλαιο, εντοπίζονται οι βασικοί κίνδυνοι που προκύπτουν από την επένδυση σε κρυπτονομίσματα, αφενός για την ομαλή λειτουργία και αποτελεσματικότητα της αγοράς και αφετέρου για τους επενδυτές. Τέλος, στο τρίτο κεφάλαιο, συνοψίζονται οι έως τώρα προσεγγίσεις κρατών και ρυθμιστικών/εποπτικών φορέων για την αντιμετώπιση των κινδύνων αυτών και παρουσιάζονται τα καίρια σημεία του Κανονισμού της Ευρωπαϊκής Επιτροπής για τα κρυπτοστοιχεία (Regulation on Markets in Crypto-Assets), του οποίου η Πρόταση δημοσιεύτηκε το Σεπτέμβριο του 2020.

## Abstract

In the last decade and after the creation of Bitcoin, the first currency based on cryptography and blockchain technology, thousands of cryptocurrencies have emerged, creating a dynamic and constantly growing investment market. In the present thesis, these unique digital assets are approached not as a means of payment but as investment products, according to the latest economic and legal developments at European and international level.

The thesis is structured in three parts. The first chapter presents the main different types of cryptocurrencies and their investment characteristics. Further, the second chapter, identifies the main risks arising from investing in cryptocurrencies, on one hand for the proper functioning and efficiency of the market and on the other hand for the investors. Lastly, the third chapter, summarizes the approaches of states and regulatory/supervisory bodies to address those risks and also the key points of the European Commission's Regulation on Markets in Crypto-Assets, the Proposal of which was published in September 2020.

## TABLE OF CONTENTS

<b>Introduction</b>	8
<b>Chapter 1: Presentation of cryptocurrencies and their use as investment products</b>	9
<b><u>Section A – Blockchain and the emergence of cryptocurrencies</u></b>	
1.1 A short description of distributed ledger and blockchain technology	9
1.2. The beginning of everything: Bitcoin	10
<b><u>Section B – Crypto-assets, categories and definitions</u></b>	
1.3 Categories of crypto-assets: cryptocurrencies and tokens	12
1.4 Types of cryptocurrencies	12
1.5 Tokens	15
1.6 “Initial Coin Offering”	16
1.7 Definitions of crypto-assets adopted by regulatory authorities and standard-setting bodies	17
<b><u>Section C – Investing in cryptocurrencies: general presentation</u></b>	
1.8 Cryptocurrencies as investment products	19
1.9 Means of transactions	20
1.10 Attractive traits of cryptocurrencies for the investors	22
1.11 Cryptocurrencies and financial inclusion	23
<b>Chapter 2: Main financial risks of investing in cryptocurrencies</b>	24
<b><u>Section A. Risks for the financial system</u></b>	
2.1 Financial crime	24
2.2 Risks associated with the means of crypto transactions	26
2.3 Liquidity risk	28
2.4 Financial institutions with crypto-assets on their balance sheet	28
2.5 Systemic Risk	29
<b><u>Section B. Risks for the investors of crypto-assets</u></b>	

2.6 Market risks	29
2.7 Operational risks	31
<b>Chapter 3: Key regulatory approaches relating to the cryptocurrency investment market</b>	<b>33</b>
<b><u>Section A. International responses to crypto-assets</u></b>	
3.1 Warnings and Guidance	33
3.2 Prohibitions	33
3.3. International standard setting and monitoring bodies	34
3.4 Anti-money Laundering: FATF Recommendations	36
<b><u>Section B. European Union approaches</u></b>	
3.5 ESMA's role and primary European law	37
3.6 Anti-money Laundering: crypto-assets under AMLD 5	38
<b><u>Section C. New legislation proposal: EU Regulation for Markets in Crypto-assets</u></b>	
3.7 Definitions under MiCA Regulation	40
3.8 Provisions concerning crypto-assets service providers	40
3.9 Provisions concerning the issuance and exchange of crypto-assets	42
<b>Conclusions</b>	<b>44</b>
<b>Appendix</b>	

## **List of Abbreviations**

<b>AMLD 5</b>	Fifth Anti-Money Laundering Directive (Directive 2018/843/EU)
<b>AML/CTF</b>	Anti-money Laundering/ Counter-Terrorism Financing
<b>BCBS</b>	Basel Committee on Banking Supervision
<b>BIS</b>	Bank for International Settlements
<b>CPMI</b>	Committee on Payments and Market Infrastructure
<b>CTPs</b>	Crypto-asset Trading Platforms
<b>DLT</b>	Distributed Ledger Technology
<b>EBA</b>	European Banking Authority
<b>ECB</b>	European Central Bank
<b>EMD 2</b>	Second Electronic Money Directive (Directive 2009/110/EC)
<b>FATF</b>	Financial Action Task Force
<b>FSB</b>	Financial Stability Board
<b>ICO</b>	Initial Coin Offering
<b>IMF</b>	International Monetary Fund
<b>KYC</b>	Know Your Customer (proceedings)
<b>MICA</b>	Markets in Crypto-Assets Regulation (Proposal/2020/EU)
<b>MIFID 2</b>	Markets in Financial Instruments Directive no. 2(2014/65/EU)
<b>P2P</b>	Peer-to-Peer
<b>PSD 2</b>	Second Payment Services Directive (Directive 2015/2366/EU)

## **Introduction**

The genesis of Bitcoin in 2008, in the midst of a global financial crisis, has eventually transformed the financial reality. The consequent emergence of thousands of new cryptocurrencies, besides the ongoing discussions about their use as a substitute for fiat currencies (i.e. means of payment in common transactions), have also shaped a brand new \$350 billion-plus market for investment products.

Cryptocurrencies, as investment products, are included in the broader category of “crypto-assets” which have caught the attention of both retail investors and regulatory authorities. Especially since the burst of Initial Coin Offerings in 2017, various issued statements from policy-making authorities were warning the public about the financial hazards these digital financial assets may entail. As a result of the highly volatile nature of their price, they often have been characterized as speculative investments. In addition, their decentralized nature and lack of control from a public authority, the constant developments in their cryptographic technology and the fact that there is not a consensus on their definition comprise the pivotal factors of them being in a grey regulatory area.

This L.L.M. thesis focuses on the use of cryptocurrencies as investment tools, examines the most significant financial risks associated with such investments and presents the material responses of international and European regulators concerning investors' protection and market integrity.

Athens, 30<sup>th</sup> November 2020

Maria S. Petraki



## Chapter 1

### **Presentation of cryptocurrencies and their use as investment products**

#### **Section A - Blockchain and the emergence of cryptocurrencies**

##### **1.1 A short description of distributed ledger and blockchain technology**

Blockchain technology is widely perceived as a technological revolution akin to the Internet's breakthrough in the late 1960s. The market has experienced significant growth over the last four years with \$1.4 billion being invested in blockchain and 2,500 patents being filed. But what exactly is blockchain?

Blockchain is the most common type of so-called *Distributed Ledger Technology* (DLT). DLT is a decentralized database managed by various participants. There is no central authority acting as an arbitrator or supervisor. Thus, all the data are distributed over a network of multiple computers instead of being stored in a central location.

DLT may be applied in a plethora of transactions: storing and moving birth certificates, votes or insurance claims. In the field of financial services, DLT allows access to a shared database for immediate clearing and settlement of securities as well as cash, without the need for the presence of any financial intermediary. Given that all the transactional information will be automatically distributed among all users, the clearing and settlement could take place almost instantaneously.

*Blockchain* can be simply defined as a series of digital information/entries (the “blocks”), related to any type of transaction (e.g. purchase of a product) and stored in a public, continuously growing decentralized ledger (the “chain”), by using cryptographic and algorithmic methods. In particular, each block comprises basic information about the relevant transactions, e.g. their date, time and value, as well as the participants, whose unique digital signatures are recorded. It also contains a “hash” i.e. a unique cryptographic code, created by a special algorithm, that differentiates it from any other block and constitutes its unique digital identity.

The blockchain process could be described as follows; a user initiates a transaction, which is represented as a “block” and broadcasted to a peer-to-peer (P2P) network of thousands or even millions of computers (also

known as “nodes”). The records of this transaction block, which are encrypted data (e.g. time, amount, user status), must afterwards be validated from the P2P network. All network participants collectively determine the block’s validity according to a pre-defined algorithmic validation method (“consensus mechanism”). Once the block is verified, the block gets a hash and, therefore, a green light to become a part of the specific blockchain of transactions. Afterwards, every participant/node adds the new verified block to their respective ledgers. This mechanism ensures that each change to the ledger is replicated across the entire network and each participant has an identical copy of the entire ledger at any point in time. The blocks are unambiguously connected. They arise through a process called "proof of work", during which the algorithmic solution of a complex computational problem is achieved.

In this way, the blockchain functions as a decentralized accounting ledger, which is common to all participants, as everyone involved keeps a copy of it. The data cannot be modified or deleted from the ledger, without the modification of the entire blockchain. This, in theory, ensures the security and transparency of the transactions and comprise the essence of the decentralized nature of blockchain: it is no longer necessary to have an intermediate "trust" authority (e.g., a bank) because the trust of the trading parties is based on algorithmic confirmation.

The first financial application of blockchain technology occurred about a decade ago with the launch of the first digital asset based on cryptography, the famous *Bitcoin*.

### 1.2. The beginning of everything: Bitcoin

It all started in November 2008, when a (still unknown to date) developer or group of developers under the pseudonym Satoshi Nakamoto published a whitepaper on the cryptography mailing list at *metzdowd.com* describing a *cryptocurrency*, named "Bitcoin: A P2P Electronic Cash System"<sup>1</sup>. With this work, Satoshi Nakamoto laid the foundations not only for Bitcoin but also for hundreds of other cryptocurrencies, which would follow and mimic the same operating form. Hence, Bitcoin is the first type of digital currency, the most representative in its operation and to date, the most important: Bitcoin currently holds the largest share in the digital currency market with a rate of 62,4% and a capitalization of 199,622 billion U.S. dollars, as of November 2020.

---

<sup>1</sup> See general: **Nakamoto**, 2008

New Bitcoins are generated through the process of *mining*<sup>2</sup>. Mining refers to the process of validating and adding transaction records to a cryptocurrency's public ledger of past transactions (i.e., the blockchain). As already mentioned, each block is an independent mathematical proof that depends on the previous block. As an incentive to update the blockchain, Bitcoin -and other cryptocurrencies- miners may collect transaction fees for the transactions they confirm, along with newly created coins (i.e., rewards). Only the first miner to compute the proof is rewarded with the coin, while the rest of the miners have to start over on an entirely new block.

It should also be noted that Bitcoin and almost all cryptocurrency transactions are executed using a two-key system. For each transaction, there is one public and one private key, both comprised of a series of numbers and letters. The private key is known only by the owner and is used to create a digital signature for a transaction. The public key, which is known to everyone on the network, serves as an address on the blockchain network and is used to verify a digital signature / validate the identity of the sender. In other words, the public key is used to receive Bitcoins while the private key is needed to digitally sign transactions to spend those Bitcoins.<sup>3</sup>

Bitcoin supply is increased with every new block of transactions that is added to the blockchain. Currently, the reward is twelve and a half (12,5) Bitcoins for each block that is added to the blockchain. The reward for solving a block is automatically adjusted so that roughly every four years of operation of the Bitcoin network, half the amount of Bitcoin created in the prior four years are created. It is understood (but not guaranteed) that the total number of Bitcoins in existence will never exceed 21 million.

Mining is currently very expensive and time-consuming, and miners must dedicate substantial resources to continuously power and cool devices. The mining reward system is designed to ensure miners are compensated for their efforts and new Bitcoin enters into public circulation. The Bitcoin network's mining protocol is intended to make it more difficult to solve for new blocks in the blockchain as the processing power dedicated to mining increases. Therefore, the Bitcoin mining process is designed to incentivize people to be efficient and use as little power as possible to create blocks and validate the transactions. Given the time and resources that must be dedicated to mining, miners "pool" their efforts and act cohesively to combine their processing power to solve blocks. These efforts are called "mining pools"—and pool members generally split any resulting rewards

---

<sup>2</sup> To make Bitcoin easier to understand, the community and Bitcoin practitioners drew a parallel with gold, calling it "digital gold". This ratio was introduced quite early in the history of Bitcoin, because it allowed its connection to a familiar asset. Thus, in proportion to gold mining, the term "Bitcoin mining" was adopted.

<sup>3</sup> Gartz and Linderbrandt, 2018, p.5

based on the processing power they each contributed to solving such blocks.

As Bitcoin grew in popularity and gained more acceptance, users began to notice some of its shortcomings. Thus, two years after Bitcoin's mining, alternative cryptocurrencies (often referred to as *altcoins*) were launched, which were improved on overall functionality, transaction speed and privacy. Altcoins use the same decentralized technology as Bitcoin but take things a step further with unique features. Ethereum, the second most popular cryptocurrency, introduced the idea of "smart contracts", i.e. self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code.<sup>4</sup> Subsequently, various new applications were developed in the crypto market.

## **Section B – Crypto-assets, categories and definitions**

### **1.3 Categories of crypto-assets: cryptocurrencies and tokens**

The application of DLT, as previously described, facilitated the use of brand new (digital) financial tools. As aforementioned, *cryptocurrencies* were the first type of these tools to emerge and *tokens* followed, gaining wide popularity through Initial Coin Offerings (ICOs <sup>5</sup>) by the end of 2017 and persisting as a trend until today. At present, the term “*crypto-assets*”, broadly described as private digital assets that use cryptography, is used to refer to a wide variety of private assets and may include both the two abovementioned categories, but also some other, hybrid forms of crypto-financial assets:

### **1.4 Types of cryptocurrencies**

#### **(a) Traditional cryptocurrencies (non-collateralized)**

Cryptocurrencies (or coins), as their name may suggest, may include functions of traditional currencies, such as the exchange on common financial exchanges and trading platforms, and also as a store of value or units of account. They can constitute, hence, a peer-to-peer alternative to fiat money<sup>6</sup>. It should be noted, though, that traditional “non-backed” up cryptocurrencies, like Bitcoin, are considered by their users “something of

---

<sup>4</sup> **Frankenfield**, Investopedia 2019

<sup>5</sup> See below, under 1.6

<sup>6</sup> Fiat money is a currency that lacks intrinsic value and is established as a legal tender by government regulation. Traditionally, currencies were based on physical commodities such as silver and gold, but fiat money is based on the credit of the economy. The value of fiat money depends on supply and demand and was introduced as an alternative to commodity money and representative money. Commodity money is created from precious metals such as gold and silver, while representative money represents a claim on a commodity that can be redeemed.

value” but they do not represent any underlying asset, claim or liability.<sup>7</sup> Thus, they are prone to high price volatility and as such, a discussion about their adoption as a counterpart of traditional currency is expected to be challenging.

However, the migration towards digital payments and digital representations of value continues to accelerate and cryptocurrencies are increasing in popularity rapidly. In particular, the outbreak of the Covid-19 pandemic has showcased the value of digital operating models and is likely to force many companies to speed up their digital innovation and transformation, including the use of cryptocurrencies in their transactions and payment systems. Evidently, there is an increased interest in digital currencies from central banks, large commercial/investment banks, funds and consumers. A recent example of this growing interest is the launch of a new service from the American payment company *PayPal Holdings Inc.* on 21 October 2020 which enables its customers to buy, hold and sell cryptocurrency directly from their PayPal account. In addition, it signalled its plans to significantly increase cryptocurrency's utility by making it available as a funding source for purchases across its global network of merchants. As of November 2020, there are more than 5.209 cryptocurrencies in the market<sup>8</sup> and market total capitalization reached almost half a trillion U.S. dollars. In general, the global cryptocurrency market is expected to continue its strong growth during the next five years.

#### **(b) Stablecoins, the asset-backed cryptocurrencies**

Given the volatile nature of cryptocurrencies' prices, there was a need to store value in something fixed, while simultaneously having the ability to transfer and buy via them. This had led to the emergence of a slightly different category of cryptocurrencies, the so-called “stablecoins”. Stablecoins are cryptocurrencies that are issued on an existing blockchain (they are not created through a new blockchain). They comprise an addition typically pegged or linked to the price of an asset, a pool of assets or a traditional currency, and therefore designed to maintain a more stable value. Unlike common cryptocurrencies which are decentralized, stablecoins include a claim against a specific issuer or some other right or interest. Depending on the type of their collateral, they can be divided into *Fiat-Collateralized Stablecoins* which maintain a fiat currency reserve - like the U.S. dollar- and *Crypto-Collateralized Stablecoins*, which are backed up by other cryptocurrencies. There are also *Algorithmic stablecoins* that are backed by users' expectations about the future purchasing power of their holdings, they are not based on any underlying asset and whose operation is primarily decentralised. In November 2020, the total value of stablecoins reached the amount of almost €20 billion, of

---

<sup>7</sup> Bullmann, Klemm and Pinna, 2019, p. 6

<sup>8</sup> Source: Coinlore [https://www.coinlore.com/all\\_coins](https://www.coinlore.com/all_coins)

which the most dominant is Tether (named so because it “tethers” itself to the value of the U.S. dollar), USD Coin and Dai<sup>9</sup>.

The arrival of stablecoins is considered to be one of the most important events that have happened in the field of cryptocurrencies, since they offer a simple and useful solution to the problem of lack of underlying assets and, therefore, of non-backed up cryptocurrencies’ highly volatile prices. It should be mentioned that stablecoins’ key elements, i.e. their decentralized/based on DLT nature on the one hand and the embodiment of a claim against an issuer, on the other hand, could drive to their comparison to security tokens<sup>10</sup>. However, they are initially different given that stablecoins are used mostly as a means of payment and exchange, whereas security tokens are used for investment purposes.

### (c) CBDCs

*Central Bank Digital Currencies (CBDCs)*, which currently have initiated a lot of discussion at an international level, comprise a kind of digital assets more similar to traditional currencies. CBDCs can be described as virtual currencies issued by a central bank for payment and settlement, in either retail or wholesale transactions for wholesale purposes, or as a complement to or a substitute for physical banknotes and coins<sup>11</sup>.

Central banks are responding to the reality that digital currencies, either privately- or publicly issued, will be an unavoidable part of the global monetary system<sup>12</sup>. Some of the world’s most influential Central banks such as the Central Bank of China, the Bank of England and the Central Bank of Sweden are working intensely on moots and test projects regarding digital currencies since 2014. As far as the Eurozone is concerned, in May 2018, a Spanish Member of European Parliament, Jonas Fernandez, has addressed a question<sup>13</sup> to the European Central Bank (ECB) about the idea put forward by some economists to issue a digital version of the euro, thus providing current accounts for people at the national central banks. ECB’s President denied such possibility, on the grounds that a) DLT/ blockchain technology had not yet been tested and required further developments before utilised by central banks, and b) that central banks managing individual accounts for families and companies would mean that the Central Bank would compete with deposits in the banking sector and would potentially pose “*substantial operational costs and risks*.”<sup>14</sup> In December 2019, the ECB nonetheless stated that “The ECB will also continue to assess the costs and benefits of issuing CBDCs

---

<sup>9</sup> Source: Coingecko <https://www.coingecko.com/en/stablecoins>

<sup>10</sup> See below, under 1.5 (b)

<sup>11</sup> **OMFIF and IBM** 2019, p.35

<sup>12</sup> *Ibid*, p. 4

<sup>13</sup> See **Fernandez** question to the ECB, 05/2018

<sup>14</sup> **ECB**, 09/2018

which could ensure that the general public will remain able to use central bank money even if the use of physical cash eventually declines”<sup>15</sup>. Nearly a year after, on 2 October 2020, ECB published a “*Report on a digital euro*”<sup>16</sup>, which examined the benefits of minting such a central bank digital currency.

In any case, there is a significant difference between cryptocurrencies and CBDCs. A CBDC is a central bank liability and a digital representation of cash, meaning that it is issued by the central bank and remains under its responsibility at all times. Simply put, the governments and central banks remain accountable to citizens for ensuring that the value of the instruments that issue is unchanged over time, either in cash or in digital currency. Cryptocurrencies, and crypto-assets in general, on the other hand, have a private nature and they are not the responsibility of any entity, so there is no reliable framework for maintaining their value and protecting their immediate holders.

### 1.5 Tokens

As abovementioned, *tokens* comprise the other main category of crypto-assets and typically represent an entitlement to an asset or a right. This is what differentiates them from cryptocurrencies -or at least traditional non-backed cryptocurrencies-, which generally do not embody intrinsic rights and entitlements. Tokens offer their holders certain economic and/or governance and/or utility/consumption rights. Broadly speaking, they may be considered as digital representations of interests or rights to (access) certain assets, products or services. Tokens are typically issued on an existing platform or blockchain to raise capital for new entrepreneurial projects, to fund start-ups (through ICO’s) or the development of new technologically innovative services. Their two main subcategories are *utility* and *security* tokens.

#### (a) Utility tokens

Utility tokens are the tokens that grant their holders access to a specific application, product or service often provided through a newly developed (blockchain-type) infrastructure. Utility tokens, unlike security tokens and shares, don’t provide the rights of ownership over a part of a company, they are just used to finance a network by providing its buyers with a guarantee of being able to consume some of the network’s products. Their main difference with cryptocurrencies is that they are not mineable and are based on third-party blockchain.

---

<sup>15</sup> ECB, 2019

<sup>16</sup> ECB, 2020

### (b) Security tokens

Security (or investment tokens) derive their value from an external, tradable asset, for example stocks or real estate. The owner of a tokenized version of a stock acquires the same rights that he would get as an owner of a stock, such as profit share and voting rights. The only difference is that a token comes in digital form. The major distinction to utility tokens is that security tokens are designed to be investments. Thus, they may fall under the same regulatory oversight as other investment products.

### 1.6 Initial Coin Offerings

Another application of blockchain technology is crowdfunding schemes based on DLTs, the *Initial Coin Offerings*. ICO is a fundraising tool for startups and facilitates the launch of new cryptocurrencies. The term ICO is inspired by the term IPO (Initial Public Offering), the name for the process whereby a private firm lists its shares on a public stock exchange. However, while in the IPO process firms are obligated to comply with costly and strict provisions prescribed by securities regulators, the ICO process has developed into an insufficient regulatory framework, often out of the scope of existing capital market legislation. That is probably the result of their purely digital nature and disconnection from traditional financial instruments and venues. Hence, ICOs usually take place without applying the rules governing the public placement of securities, such as eligibility or prospectus requirements and without the involvement of traditional financial intermediaries. Recently, the popularity of this method has established it as a major source of capital for start-ups. Since the completion of the first ICO - by Omni Layer (also known as Mastercoin) in 2013 and Ethereum in 2014 - many have followed. In 2020, more than \$ 3,2 billion were raised from digital currency sales to investors alone. Two new start-ups, Filecoin and Tezos, are the largest offerings to date, at \$ 275 million and \$ 232 million respectively.

*Tokens* are pivotal to this model of financing. A token provides a key to its owner that unequivocally certifies that the person who owns it, also owns something of value. As already mentioned, tokens, which may be backed up by/ assigned to physical assets, can be utilized by their owners for obtaining a service or a share in a platform. Participation in such processes requires the purchase of tokens using fiat currency (e.g. euro) or acceptable cryptocurrency (e.g. Bitcoin, Ethereum). Tokens are available in a blockchain database which is considered to ensure transparency, transaction certification and control by the network community or any interested party. Depending on the case, certain standards are followed, so that tokens have exchangeable or interoperable characteristics. The most common technical standard is the ERC 20 of the Ethereum platform.

Token holders are promised a share of the financed platform (similar to traditional equity investing without the element of holding tangible



assets/securities). Sold tokens serve as participation tickets to the platform. For example, a token may represent a digital currency, 1% of a painting, a part of real estate etc. The various applications of tokens in sectors of the economy extend the possibility of financing and supporting goods and their owners (asset owners) which are not -yet- marketable. It also provides flexibility in acquiring them, as an investor or supporter can buy a small fraction of the good, and then exchange it.

### 1.7 Definitions of crypto-assets adopted by regulatory authorities and standard-setting bodies

At the moment the crypto market is continuously evolving, thus there is still no generally accepted definition of what constitutes a crypto-asset. This often results in an overlap between the commonly used terms, such as “crypto-asset”, “cryptocurrency”, “crypto token”, “virtual currency” and “digital asset”/ “digital currency”.

Regulatory authorities and standard-setting bodies in Europe and around the world, based on the characteristics of the different categories of crypto-assets as already described, have attempted to define the term for their monitoring and supervisory work.

The following definitions are found in the most recent (starting from 2018) relevant papers of the international for a/policy making authorities, which try vigorously to keep pace with the international investment developments in crypto markets.

**Financial Stability Board (FSB)** has defined the term as “*a type of private digital asset that depends primarily on cryptography and distributed ledger or similar technology*”, whereas it defines a digital asset as “*a digital representation of value which can be used for payment or investment purposes. This does not include digital representations of fiat currencies*”<sup>17</sup>. The same definition is also adopted by the **Committee on Payments and Market Infrastructures (CPMI)**<sup>18</sup> ;

**International Organization of Securities Commissions (IOSCO)** enriches the abovementioned description, defining 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. Crypto-assets can represent an asset or ownership of an asset, such as a currency, commodity, security, or a derivative on a commodity or security*”<sup>19</sup>;

---

<sup>17</sup> FSB, 05/2019, p.10

<sup>18</sup> CPMI, 10/2019, p.1

<sup>19</sup> IOSCO, 02/2020, p. 1

A similar line is followed by the **European Securities Markets Authority (ESMA)** which defines a crypto-asset as “*a type of private asset that depends primarily on cryptography and DLT as part of its perceived or inherent value*”. This definition pertains to both virtual currencies and digital tokens issued through ICOs. ESMA also clarifies that “*a crypto-asset means an asset that is neither issued nor guaranteed by a central bank.*”<sup>20</sup> ;

**European Banking Authority (EBA)** defines the term 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*”<sup>21</sup>;

**International Monetary Fund (IMF)**, in October 2020, has defined the term as “*digital representations of value, made possible by advances in cryptography and distributed ledger technology*”<sup>22</sup>;

**European Central Bank (ECB) Crypto-Assets Task Force** refers to crypto-assets 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*”. This definition isn’t broad enough, since it seemingly includes only traditional cryptocurrencies which are not collateralized and excludes security tokens or stablecoins.

**European Commission** in its proposal Regulation dated 24.09.2020<sup>23</sup>, gives a definition as broad as the one given by IMF, which, may cover the majority of this new generation of assets: “*crypto-asset’ means a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology*”.

It may be observed that the similar components in the above definitions are, a) the underlying use of cryptography, DLT or similar technology and b) the private nature of the asset. 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.

For the purpose of this study, the use of the term “cryptocurrency” will refer to traditional, non-backed cryptocurrencies and will be focused on their investment nature -not on their potential role as means of payment. Additionally, the term “crypto-asset” will refer to all these digital assets

---

<sup>20</sup> **ESMA**, 01/2019, p. 42

<sup>21</sup> **EBA**, 01/2019, p. 11

<sup>22</sup> **IMF**, 2018, p. 4

<sup>23</sup> See below, in Chapter 3

that: i) are transferred and stored electronically, on the basis of cryptography, DLT or similar technology, ii) are not issued/guaranteed by a central bank or a public authority, iii) represent a value and iv) are used as investment assets, i.e., financial assets purchased with the expectation that will provide income further or will later be sold at a higher cost price for a profit.

## **Section C – Investing in cryptocurrencies: general presentation**

### **1.8 Cryptocurrencies as investment products**

Since the first mining of Bitcoin in 2008, the position of cryptocurrencies in the financial landscape has changed radically. Their use as investment products has shifted the discussion about a new kind of currency and transaction network to asset and portfolio management. Their significant price growth and volatility, especially toward the end of 2017 (when the total number of cryptocurrencies and digital assets on exchanges skyrocketed from 617 to 1,335 over the course of the year) an increasing number of individual investors have chosen to participate in the crypto market. Warnings from the supervisory authorities advising against “buying, holding or selling virtual currencies” haven’t seemed to dwindle retail investors’ appetite to allocate capital in this new asset class. Retail investors’ risk appetite has rebounded somewhat post the recent international financial crisis of 2007-2009, creating appealing market dynamics for cryptocurrencies. On the other hand, institutional investors have been monitoring the asset class for several years given the scepticism around the downside risks and the associated risks pertaining to the risk tolerance of their mandate. Notwithstanding, there has been a wave of asset managers, predominantly wealth managers, that recently invested in the space which is somewhat reflective of their opportunistic mandate as well as their need for portfolio diversification. The main driver behind the increased demand is the institutionalization of crypto-related products. The latter includes direct investments in cryptocurrencies as well as the trading of crypto futures in the Chicago Board Options Exchange. In addition, there is a variety of active and passive investment strategies/funds which are dedicated to crypto-assets. Passive investments pertain to designing indices for crypto-assets prices and the launch of exchange-traded products (ETPs) that track the value of these indices (e.g. XBT provider by Coinshares). Active funds comprise largely long-only offerings spanning for Bitcoin-focused strategies to blockchain-related strategies (e.g. Pantera’s Blockchain Investment Fund) with complementary strategies being short crypto strategies (through futures or margin lending), crypto lending (e.g. CoinLoan) and crypto trade finance.

## 1.9 Means of transactions

### (a) Centralized Exchanges

The most common means that investors use to buy and sell cryptocurrency holdings are the *Centralized Exchanges* (CEs), of which the most widely used is Coinbase and Binance. CEs are online trading platforms that are not built on decentralized blockchain infrastructure but instead represent blockchain-based assets within an internal database, controlled only by them. When investors buy cryptocurrency, for example Bitcoin, on a CE, they are buying a representation of it within the exchange's database and they only come to own actual Bitcoin when they withdraw it from the exchange's wallet to a wallet whose private key they control. Until that point, the CE has custody of their Bitcoin – and the user is trusting them to keep it safe.

This centralized, custodial system has certain advantages. For instance, blockchains are not compatible with each other (for example Ethereum cannot “be connected” directly to Bitcoin), which means that some intermediary system is required to trade assets across different chains. Hence, CEs facilitate a Forex type of trading for crypto-assets an easy way of bringing Forex-like trading to crypto-assets. It is claimed, though, that CEs undermine crypto-assets' decentralized nature, which constitutes their key element and a major driver of their value. As trusted parties, CEs are targets for hackers and huge amounts of money continue to be stolen, even from some of the largest, most established exchanges. At the same time, they remain totally non-transparent and there is evidence to believe that manipulation occurs within their matching engines.

(b) Decentralized Exchanges (DEs), by contrast, are built using blockchain infrastructure. A genuine DE will be non-custodial, never taking control of users' assets and allowing them to trade directly from a wallet they control. Owing to the limitations of building directly on blockchains, existing DEs exhibit much poorer performance and user interfaces than CEs, hence their relative unpopularity. They are harder to use and have difficulties solving front-running problems. DEs are also unable to offer trading across chains without some form of a custodial solution, e.g. creation of a representation of a coin or a token on another, compatible chain.

In general, cryptocurrency exchanges offer their users a wide range of payment options, such as wire transfers, PayPal transfers, credit cards and also a variety of coins.<sup>24</sup>

---

<sup>24</sup> Houben and Snyers, 07/2018, p. 26

### (c) Crypto wallets

A crypto wallet is a program used for interactions within a blockchain network. Crypto wallets don't store the cryptocurrency holdings but act as a tool of connection with the blockchain, by generating the necessary information to receive and send money via blockchain transactions. In essence, they store the user's private and public cryptographic keys, which are necessary to get access to the blockchain on the user's behalf and make transactions with his/her cryptocurrency. Based on these keys, an alphanumeric identifier, called *address*, is generated: the public key is like an address for each user's wallet, whereas the private key is an address used to unlock it. For a transaction to occur between two users, one needs to know the public key of the other in order to reassign the money between their addresses. To do so, the sender needs at the same time access to his/her own private key. In turn, to unlock and spend new funds, the receiver must enter the private key that corresponds to his/her public key. Basically, a wallet is only comprised of two keys and coins are just transferred from one address to another, never leaving the blockchain. The address can be shared to receive funds, but private keys are to be never disclosed. When a transaction occurs, the only thing that actually happens is the addition of a block describing the transaction to the blockchain.<sup>25</sup>

The three major types of crypto wallets are *paper, software and hardware, wallets*. Based on their operations, they can be further classified as cold or hot wallets.

The simplest and most basic form of cryptocurrency wallet is the *paper wallet*. As the name suggests, a paper wallet is a user's private and public key set, either written or printed on a piece of paper which usually includes a QR code.<sup>26</sup> If printed, the user can also include his/her wallet's QR code for easy scanning to add additional funds. This type of wallet is also referred to as a *cold storage* wallet because the private keys are not accessible via the internet.

However, paper wallets can only store cryptocurrency, that's why they are considered unreliable and obsolete. In order to proceed to a payment, the user will have to create another type of wallet, and transfer funds from the paper wallet to the new one.

*Software wallets* (also known as hot wallets) are software or apps that manage the user's cryptocurrencies and can be downloaded to a computer or a mobile device. Some are designed to be used with just one cryptocurrency while others have support for many different crypto-assets. Finally, there are the *hardware wallets* i.e., hardware devices that individually handle public addresses and keys and look like a USB with OLED screen and side buttons. They are considered by far the most secure

---

<sup>25</sup> See general Sharma-Blockchain Council, 2020

<sup>26</sup> Source: BitGear <https://www.bitgear.com.au/>

method of storing cryptocurrencies because the private keys for each wallet are encrypted on the device and cannot be exported. Also, any transaction made on a hardware wallet must be confirmed by pressing physical buttons on the device. Hence, the possibility of a hacker or virus being able to steal a user's private key or make transactions from his/her wallet without his/her knowledge or approval is very limited.

#### 1.10 Attractive traits of cryptocurrencies for the investors

**Risk-Return Reward:** Historically, cryptocurrencies have experienced sharp fluctuations in value. Without a doubt, high price volatility is the riskiest feature of non-backed cryptocurrencies, but it may comprise simultaneously one of their most attractive investment features, considering the upside potential. Large volatility seems at the same time a possibility of significant appreciation in the future. Bitcoin's price, for instance, in only one year almost doubled (starting with a price of €6,000 in November 2019 and reaching €15,650 in November 2020, getting closer to its highest price ever recorded, €16,670 in December 2017<sup>27</sup>).

**Decentralized nature:** Peer-to-peer operation of cryptocurrencies frees from third-party oversights, reduces the high cost of transaction fees and allows investors to overcome middlemen. This further enhances the security features by eliminating the risk of an untrustworthy middleman. Moreover, monetary policy dictated by central banks can cause a devaluation of centralized currencies, whereas, cryptocurrencies are not subject to the will of central banks and are only determined by market dynamics.

**Inflation Hedge:** One of the main advantages of investing in cryptocurrencies is that they can serve as a hedge against traditional money, which is vulnerable to inflation issues. Most cryptocurrencies are inflation neutral because they have hardcoded limits on how many share units can be issued. The common example is, as already mentioned, the 21 million units hard limit of Bitcoin. No more coins can ever be issued, unless the crypto-asset is modified ("forked"<sup>28</sup>) by a coder, essentially resulting in a new cryptocurrency with different parameters.

**Security:** As already mentioned, each transaction involving cryptocurrencies is transparently stored in a distributed public ledger (blockchain). These blockchains are visible to all users, both participating and non-participating in the transaction. The creation of new blockchains demands from the maintained miners to solve

---

<sup>27</sup> Source: Coindesk <https://www.coindesk.com/price/Bitcoin>

<sup>28</sup> See below, under 2.7

extremely complex computational problems that require a considerable amount of computing. As such, for anyone to manage to corrupt the process, an over 51% control of the details of the total blockchain network is required, something that is redundant, fruitless and almost impossible. Another positive is the anonymity factor, given that the names of the traders are not displayed except for a code corresponding to their public key.

### 1.11 Cryptocurrencies and financial inclusion

According to the World Bank<sup>29</sup>, around 1.7 billion people, mainly from the global south in continents such as Asia and Africa, do not have access to regular banking accounts. Many of the world's population remains unbanked largely due to economic hardship, insufficient banking and governmental infrastructures or financial illiteracy. At the same time, there is a lack of effort from financial institutions to solve these issues, because they often consider this part of the population is unprofitable. The use of cryptocurrencies could theoretically help to mitigate some of the above issues. Unlike a bank, there is a very low barrier of entry in a cryptocurrency transaction and, since everything is done via the internet, distance stops being an issue. Anyone can be a crypto investor, as long as he/she has a stable internet connection and can buy, sell and use cryptocurrencies. Also, the decentralized nature of crypto transactions could eliminate intermediation and its high fees, which for unbanked groups of the population may be unbearable. Moreover, in many developing countries it is difficult to acquire identity documents due to their cost, or the lack of administrative infrastructures. Cryptographic design, on which cryptocurrency transactions are based, would not require the typical legacy documentation and would enable billions of people to become easily identifiable on a public blockchain.

Given that many people, especially those living in developing regions, cannot access the traditional banking system, the opportunity to earn, save and invest in cryptocurrencies, by the use of just their mobile phones is greatly beneficial. The dire economic state in some countries around the world (like Venezuela) has already caused many citizens to turn to cryptocurrency as an alternative investment.

---

<sup>29</sup> Source: <https://globalfindex.worldbank.org/>

## Chapter 2

### Main financial risks of investing in cryptocurrencies

Despite the constantly increasing popularity of investing in cryptocurrencies, the area is subject to multiple risks that differ in both degree and nature from conventional capital market risks. These risks are either concerning the investors or the financial system in which the investment transactions take place.

#### Section A. Risks for the financial system

##### 2.1 Financial crime

Trading cryptocurrencies and crypto-assets, in general, are associated with serious dangers of criminal activity (or “crypto-crime” as some put it). Concerns of financial regulators, legislators and law enforcement agencies have focused on the pseudonymous and decentralised nature of these assets and therefore the difficulty in tracing payments, which may contribute to criminal activity such as money laundering, tax evasion and terrorist financing.

The most significant of the features that make cryptocurrencies attractive to criminals is their *anonymity*, which may allow shady transactions to occur outside of the regulatory perimeter. While conventional payments can, in theory, be traced to an internet public key address, in crypto transactions the public key is not linked to a particular individual. Trading account information and the identity of the owner are not tied to the crypto-asset itself, making the tracing of payments difficult. Hence, the trading of cryptocurrencies via crypto-trading platforms provides criminals or criminal organizations with easy access to “clean cash” (both cash in/out) anonymously.

**(a) Money laundering:** Cryptocurrencies are used for *money laundering* purposes, mainly due to a lack of robust Know Your Client (KYC) measures implemented by traditional banking institutions and trading platforms of other financial assets. Indicative of the popularity of money laundering proceeds in this area is that numerous crypto-trading platforms allow cryptocurrencies to be traded with cash without any further control. The transaction fee on these platforms is on average 10-15% of the total value, a rate much higher than the typical 1-2% charged by authorised exchanging platforms. In essence, the platforms allow individuals with large amounts of cash, possibly illegally acquired, to convert their cash into cryptocurrency anonymously. Once the transaction is confirmed, the



seller receives the number of cryptocurrencies, while in most cases no KYC information is required for the transaction to be completed. Through this process, the buyer can successfully complete the placement of legitimate income, derived from illegal activities, and introduce "clean" cash into the financial system. However, the usefulness of a cryptocurrency for such purposes will depend on how much record-keeping the platform mechanism maintains about the transactions, how involved the third-party service providers are in the transactions and whether such third parties comply with anti-money laundering requirements.

**(b) Fraud cyberattacks:** The lack of identity information in the scope of cryptocurrency trading, places often these decentralized transactions on the target of fraud attacks. A usual fraud method is similar to "pump and dump" or the Ponzi scheme. The execution of this scam is relatively simple: a cryptocurrency is artificially inflated in value in order to attract investors and create the illusion of a worthwhile and profitable investment. This is possible because new investors' money is used as a return on interest from previous investors, creating a vicious circle where "profits" are nothing more than the capital of new investors. At any time the perpetrators of the fraud extract the largest possible amount of money and disappear. The more they manage to maintain the illusion of solvency in this "bubble" investment, the more capital they accumulate, which can then be used to attract new investors and aggravate fraud. Although these scams are well known in the traditional financial system, when they are carried out through cryptocurrencies it is even more difficult to identify.

**(c) Tax evasion:** In addition, since there is no disclosure of participants' identity and crypto transactions can take place easily and very quickly across borders, the investment income cannot be easily traced and a wide space for *tax evasion* is created. Entering into taxable cryptocurrency transactions without paying taxes comprises tax evasion. A tax authority does not know who enters into the taxable transaction, because of the anonymity involved, and therefore, it cannot detect nor sanction this<sup>30</sup>. Also, due to the changeable nature of these assets, the classification of their transactions (for example in relation to the length of the holding period, the speculative character of the transaction or the treatment of cryptocurrencies as capital assets instead of currencies) would depend on the applicable tax rules in the relevant jurisdiction. This can also lead to regulatory arbitrage.

---

<sup>30</sup> Houben and Snyers, 07/2018, p. 53.

(d) Frauds related to ICOs: The lack of regulation around Initial Coin Offerings in most countries has facilitated the appearance of information asymmetry, which in some cases may lead to huge frauds against ICOs' investors. At ICOs, criminals may make a public call to attract investors to support a new company or venture, similar to the way a regular company issues shares when it goes public. Investors buy shares in the company through cryptocurrencies and expect a share of its profits. But often these companies do not even exist in reality and the ventures are just ideas without any substantial implementation plan. Hence, it is enough for criminals to persuade willing investors to buy a large number of coins at ICOs, which do not correspond to the real value of the company or the venture and then disappear with the amount they have collected.

## 2.2 Risks associated with the means of crypto transactions

(a) Unregulated crypto exchanges: Venues through which cryptocurrencies are exchanged are new and, in many cases, largely unregulated. The vast majority of decentralized exchanges or over-the-counter trading venues do not provide the public with significant information regarding corporate practices, regulatory compliance or ownership structure. As a result, the marketplace may lose confidence in or may experience problems relating to crypto-trading platforms. In particular, these platforms may impose daily, weekly, monthly or customer-specific transaction or distribution limits or suspend withdrawals entirely, rendering the exchange of cryptocurrencies for fiat currency difficult or impossible. Consequently, participation in crypto-trading venues requires users to take on credit risk by transferring digital assets from a personal account to a third party's account.

Over the past several years, several crypto exchanges have been closed due to fraud, failure or security breaches. In many of these instances, mainly due to lack of regulation, the customers of such exchanges were not compensated or made whole for the partial or complete losses of their account balances on the exchanges. While smaller crypto exchanges are less likely to have the infrastructure and capitalization that make larger crypto exchanges more stable, larger crypto exchanges are more likely to be appealing targets for hackers and "malware" (i.e., software used or programmed by attackers to disrupt computer operation, gather sensitive information or gain access to private computer systems). A large loss incident occurred in 2014, when the largest Bitcoin exchange at the time, Mt. Gox, filed for bankruptcy in Japan amid reports the exchange lost up to 850,000 Bitcoins, valued then at over \$450 million.<sup>31</sup> Even in cases where compensation was ultimately fully paid out within several months, investors were not able to use their hacked cryptocurrencies or tokens over

---

<sup>31</sup> Cuervo, Morozova, Sugimoto, IMF, 12/2019, p. 3

extended periods. Some exchanges are trying to mitigate this risk by contracting cyber insurance coverage or by creating separate compensation funds, but there is typically no public or other safety nets, such as deposit insurance or a liquidity facility from central banks.<sup>32</sup>

**(b) Regulated crypto exchanges:** On the other hand, typically regulated crypto exchanges must comply with minimum net worth, cybersecurity, and anti-money laundering requirements, but are not typically required to protect their investors to the same extent as regulated securities exchanges or futures exchanges are required to do so. For instance, crypto exchanges in the U.S.A. are not currently obligated to comply with either state or federal requirements such as prevention, detection and reporting of manipulative trading activity. However, in February 2018, the New York State Department of Financial Services (NYDFS) issued a guidance<sup>33</sup> that directed “virtual currency entities” to adopt a written policy to address fraud-related and similar risk areas, including inter alia market manipulation, effective procedures and controls and investigation procedures in the case of suspected -or actual- fraud.

Furthermore, many cryptocurrencies exchanges lack certain safeguards put in place by more traditional exchanges to enhance the stability of capital markets and prevent flash crashes, such as limit-down circuit breakers.<sup>34</sup> As a result, the prices of cryptocurrencies on crypto exchanges may be subject to larger and/or more frequent sudden declines than assets traded on traditional exchanges. For example, on June 21, 2017, at approximately 3:30 p.m., the price of Ethereum on the Coinbase Pro exchange declined from \$317.81 to \$0.10 and then recovered to prices above \$300, all within the span of approximately 10 seconds.

A lack of stability in crypto exchanges, manipulation of crypto markets by crypto exchange customers and the closure or temporary shutdown of such exchanges due to fraud, business failure, hackers or malware, or government-mandated regulation, may reduce confidence in the cryptocurrencies generally and result in greater volatility in their market price.

**Custodian wallet risk:** Having cryptocurrencies on deposit or with any third party in a custodial relationship has attendant risks including also security breaches, risk of contractual breach, and risk of loss. An investor may have a high concentration of its cryptocurrencies in one location or

---

<sup>32</sup> Coinbase, for example, has insurance coverage of all client positions held in its hot wallet by a large reinsurer. If Coinbase were to suffer a breach of its online storage, the insurance policy would cover any customer funds lost as a result.

<sup>33</sup> See general NYDFS, 02/2018

<sup>34</sup> Source: Liepajasjv, 10/2020

with one third party wallet provider, which may be prone to enormous losses arising out of hacking, loss of passwords, compromised access credentials, malware, or cyber-attacks.

### 2.3 Liquidity risk

(a) In the context of cryptocurrencies, liquidity refers to the ability of a cryptocurrency to be converted into cash or other cryptocurrencies easily, i.e., their utility as a viable medium for transactions. Probably, the main factor that affects liquidity in the cryptocurrency market is the fact that the majority of cryptocurrencies' owners invest and trade coins for price appreciation rather than use them as a medium-of-exchange. Volume refers to the number of cryptocurrencies that have been traded in exchanges usually in the past 24 hours timeframe. Essentially, the volume reflects the market activity of a specific cryptocurrency; a higher volume indicates that more people are buying and selling the crypto-asset.

Furthermore, liquidity risk can be associated with the issuers of cryptocurrencies and tokens, as well as with the service providers of crypto transactions. Short term redemptions into other currencies or assets may be allowed by issuers of crypto-assets. In addition, investors may expect that they would be able to exchange the coins and tokens with service providers (such as CEs) frequently, without material redemption cost. Both the issuer and the service provider have a strong incentive to meet redemption requests from investors, in order to avoid reputation failure of the cryptocurrency or token. Such frequent redemptions could drive to fire sales of the collateral assets (such as bonds and bank deposits) by the issuers and service providers, which might have a negative impact on the broader financial sector, such as banks and bond markets.

### 2.4 Financial institutions with crypto-assets on their balance sheet

Currently, there are many jurisdictions that do not prohibit financial institutions, including investment firms, credit, payment and e-money institutions, from holding or being exposed to crypto-assets such as non-backed cryptocurrencies. However, it seems that there are only a few financial institutions that have acquired crypto-assets and their exposure to such assets remains limited<sup>35</sup>. But the potential inclusion of such assets as on balance sheet items may jeopardize their health and performance metrics (due to price volatility) as well as the broader financial system's stability, due to the inherent interconnectedness of its institutions. The BCBS and EBA have recently expressed the view that if banks do decide to acquire crypto-assets or provide related services, they should apply a

---

<sup>35</sup> See BCBS, 2019, p. 8, EBA, 2019, p. 23-24

conservative prudential treatment to such exposures, especially for high-risk crypto-assets<sup>36</sup>. EBA 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, i.e., the CRD/CRR.

## 2.5 Systemic Risk

Crypto-asset providers, such as trading platforms are gradually engaging with traditional financial institutions through derivatives, providing crypto linked products or, as aforementioned, through cyber insurance. These exposures could trigger contagion risks to financial institutions if the size of the exposures continues to grow in the future or if the risk is not managed properly. Besides, crypto-assets and DLT applications might affect the industry landscape and increase competition in the future, which may, in turn, affect the soundness of the existing financial sector. However, according to standards setters' recent assessments, crypto-assets do not yet pose material systemic risk, due to their limited use.

## Section B. Risks for the investors of crypto-assets

Crypto investors may be exposed to a significantly higher risk of loss than those investing in traditional financial assets. The risks facing the investors of cryptocurrencies could be grouped into the following two basic categories: market and operational risks. The latter category is profoundly broader, because of the complex technology that cryptocurrencies/crypto-assets are based upon, and due to their decentralized nature.

## 2.6 Market risks

**(a) Price volatility:** Financial analysts can almost accurately predict the value of real currencies or stock quotes based on data analysis. As already mentioned, trading prices for (non-backed) cryptocurrencies have historically been highly volatile and their cost fluctuations are completely unpredictable in the short term. The main reason behind this is that these assets have zero intrinsic value and, as a result, they derive value only from the belief that they might be exchanged for other goods or services, or a certain amount of fiat currency, in the future. Speculators and investors who seek to profit from trading and holding a specific cryptocurrency generate a significant portion of this cryptocurrency demand. Speculation regarding future appreciation in its value may inflate and make the price

---

<sup>36</sup> See **BCBS**, 2019, p.1 EBA, 2019, p 27.

of the coin even more volatile. By all means, changing investor confidence in future appreciation in the price of an asset associates it with high risk. Additional factors causing the variability of the value of a cryptocurrency are the large volumes of exchange trading and changing legislative initiatives of regulatory bodies (legal risk).

**(b) Miners' incentives:** Miners generate revenue from both newly created cryptocurrencies, known as the “block reward” and from fees taken upon verification of transactions. In case the aggregate revenue from transaction fees and the block reward is below a miner's cost, the miner may cease operations. If the award of new units of crypto-assets such as Bitcoin and Ethereum for solving blocks declines and/or the difficulty of solving blocks increases, and transaction fees voluntarily paid by participants are not sufficiently high, miners may not have an adequate incentive to continue mining and may cease their mining operations. For instance, the currently fixed reward for solving a new block on the Bitcoin network is six and a half Bitcoins per block, which decreased from twelve Bitcoins in 2016.<sup>37</sup> It is estimated that it will halve again in about four years. This reduction may result in a reduction in the aggregate hash rate of the Bitcoin network as the incentive for miners decreases. Miners ceasing operations would reduce the collective processing power on the network, which would adversely affect the confirmation process for transactions (i.e., temporarily decreasing the speed at which blocks are added to the blockchain until the next scheduled adjustment in difficulty for block solutions) and make crypto-asset networks more vulnerable to a malicious actor or botnet<sup>38</sup> obtaining sufficient control to manipulate the blockchain and hinder transactions. This reduction in confidence in the confirmation process or processing power of a crypto-asset network may adversely affect the total investment in the specific cryptocurrency.

Furthermore, miners have historically accepted relatively low transaction confirmation fees. If miners collude in an anti-competitive manner to reject low transaction fees, then a crypto investor could be forced to pay much higher fees. Since mining occurs globally and anonymously, it may be very difficult for authorities to apply antitrust regulations across multiple jurisdictions. Hence, any collusion among miners may impact the attractiveness of a crypto-asset network and therefore the investment in it.

**(c) In particular: Risks for the investors of crypto futures**

---

<sup>37</sup> The rewards for Bitcoin mining are reduced by half every four years. When Bitcoin was first mined in 2009, mining one block would earn 50 BTC. In 2012, this was halved to 25 BTC. By 2016, this was halved again to 12.5 BTC. On May 11, 2020, the reward halved again to 6.25 BTC, - Investopedia, E. Hong, November 2020

<sup>38</sup> Botnet: a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam messages.

Unlike the futures market for traditional physical commodities, the market for exchange-traded cryptocurrencies futures contracts (e.g. Bitcoin or Ethereum futures) has a limited trading history and operational experience<sup>39</sup> and may be riskier, less liquid, more volatile and more vulnerable to economic, market and industry changes than more established futures markets. The liquidity of the market will depend on, among other things, the adoption of the relevant cryptocurrency and the commercial and investors' interest in the market for the ability to invest in and hedge against its price with exchange-traded crypto futures contracts. Nevertheless, there is no assurance that a liquid market for crypto futures contracts will develop and the lack of such a market for these derivatives would result in high-risk investments. In addition, the cryptocurrencies centralized exchanges are not subject to typical stock and commodity market trading hours. As a result, the price of a cryptocurrency may fluctuate significantly during periods when its futures contract trading is unavailable. This conflict in trading hours may result in the trigger of price movement limits and/or decoupling of the cryptocurrency price from the value of crypto futures contracts.

## 2.7 Operational risks

**(a) Irreversibility of transactions:** The loss or destruction of a private key required to access crypto-assets may be irreversible. As already mentioned, cryptocurrencies, and all crypto-assets, are controllable only by the possessor of both the unique public key and private key or keys relating to the address on the blockchain where such crypto-assets are held. Private keys must be safeguarded and kept private in order to prevent a third party from accessing the crypto-asset while held at the corresponding address. To the extent a private key is lost, destroyed or otherwise compromised and no backup of the private key is accessible, the user will be unable to access the asset held at such address on the blockchain. The decentralized nature of crypto transactions places the risks associated with the failure of a transaction on the users of the system. This approach differs fundamentally from a centralized payment system where the central authority would assume and mitigate this risk.

**(b) Flawed cryptographic code:** In the past, flaws in the source code for cryptocurrency transactions have been exposed and exploited, including those that exposed users' personal information and/or resulted in the theft of users' digital assets. Several errors and defects have been publicly found and corrected, including those that disabled some functionality for users

---

<sup>39</sup> The Chicago Board Options Exchange (CBOE) offered the first Bitcoin future contract on December 10, 2017

and exposed users' personal information. Discovery of flaws in, or exploitations of, the source code that allow malicious actors to take or create money in contravention of known network rules have occurred. In addition, the cryptography underlying a crypto-asset could prove to be flawed, ineffective or potentially insufficiently tested, or developments in mathematics and technology, including advances in digital computing, and quantum computing, could result in such cryptography becoming ineffective. In any of these circumstances, if the investor holds the affected crypto-asset, a malicious actor may be able to steal it.

(c) "Fork" of the network: Some cryptocurrencies are open-source since any user can download their software, modify it and then propose that the users and miners of the asset adopt the modification. When a modification is introduced and a substantial majority of users and miners consent to the modification, the change is implemented and the network operates uninterrupted. However, for this to happen, a significant majority of users and miners have to consent to the proposed modification. If the modification is not compatible with the prior version of the software, the result would be a so-called "*fork*" of the network, meaning that the one part would be running the pre-modified software and the other part would be running the modified software. Consequently, two different versions of the crypto-asset would run in parallel, yet lacking interchangeability. Forks may occur after a significant security breach. For example, in June of 2016, a smart contract using the Ethereum network was hacked, which resulted in most participants in the Ethereum ecosystem electing to adopt a "hard fork" that effectively reversed the hack. Nevertheless, a minority of users continued to develop the old blockchain, now referred to as "Ethereum Classic" with the crypto-asset on that blockchain now referred to as Classic Ether, or ETC. Classic Ether remains traded on several digital asset exchanges.

(d) Internet disruption: Many cryptocurrencies are dependent upon the internet. A significant disruption in internet connectivity could disrupt a cryptocurrency's network operations until the disruption is resolved and have an adverse effect on its price. In particular, some crypto-assets have been subjected to a number of denial-of-service attacks, which have led to temporary delays in block creation and in the transfer of the assets. While in certain cases in response to an attack, an additional "hard fork" has been introduced to increase the cost of certain network functions, the relevant network has continued to be the subject of additional attacks. Moreover, it is possible that as cryptocurrencies increase in value, they may become bigger targets for hackers and subject to more frequent hacking and denial-of-service attacks.



## Chapter 3

### **Key regulatory approaches relating to the cryptocurrency investment market**

#### Section A. International responses to crypto-assets

3.1 Warnings and Guidance: Central banks and anti-money laundering authorities around the world were mostly the first to react to the emergence of crypto-assets (Bitcoin and other cryptocurrencies, in particular). Various government statements and warnings about the hazards of investing in cryptocurrency markets, regarding market integrity and investor protection, were issued. In fact, at least 102 countries have issued warnings on cryptocurrencies and on ICOs. Monetary Authority of Singapore, for example, in December 2017 published a warning encouraging “extreme caution” in regard to the “significant risks” taken when buying into cryptocurrencies and stated that prices of cryptocurrencies are “driven by speculation”<sup>40</sup>.

Such warnings were largely aimed to educate the public about the difference between traditional currencies, issued and guaranteed by a public authority and cryptocurrencies. They pointed out the risks that may result from cryptocurrencies’ high volatility, as well as from the insufficient regulation around entities that facilitate crypto transactions. Most also highlighted that investors of cryptocurrencies should be aware that they carry personal risk, and that no legal recourse is available to them in the event of a loss.

3.2 Prohibitions: Some jurisdictions have gone even further and imposed restrictions on investments in cryptocurrencies. Hence, some of them, such as Qatar, Morocco, the Republic of Macedonia, Nepal, Colombia and Maldives imposed a total ban on crypto transactions. In particular, the Qatar Financial Centre Regulatory Authority has imposed a ban on all crypto-asset services in the Gulf region. A statement in January 2020 specified that the ban will cover “anything of value that acts as a substitute for currency, that can be digitally traded or transferred and can be used for payment or investment purposes.”

Nevertheless, even though cryptocurrencies have not been legally acceptable as a substitute for any country's legal tender until now, not all countries see the advent of blockchain technology and cryptocurrencies as

---

<sup>40</sup> MAS, 12/2017

a threat. In fact, there are countries that recognize the potential in the technology behind it and are developing a cryptocurrency-friendly regulatory regime as a means to attract investment in technology companies that excel in this sector. This regime concerns mainly taxation and anti-money laundering (AML) rules. For instance, cryptocurrencies are viewed as commodities under the tax law of Canada. That means that “any income from transactions involving cryptocurrency is generally treated as business income or as a capital gain, depending on the circumstances.”<sup>41</sup> Similarly, the Financial Conduct Authority in the United Kingdom implements taxation rules on investment transactions in cryptocurrencies.

### 3.3. International standard-setting and monitoring bodies

Numerous reports and guidance regarding crypto-asset risks were also issued from international standard setters and coordination/monitoring bodies.

IOSCO: In January 2018, IOSCO’s Board released a communication regarding the risks related to ICOs, which described as “*highly speculative investments*”<sup>42</sup>, and in parallel created an ICO Consultation Network through which its members can exchange their experiences and concerns, including any cross-border issues.

Also, in February 2020, the Board published a report that describes the issues and risks associated with crypto-asset trading platforms (CTPs). The report sets out key considerations to assist regulatory authorities in addressing issues regarding the operations of these platforms, such as transparency, identification and management of conflicts of interest, price discovering mechanisms, safekeeping of assets and technology resiliency<sup>43</sup>. In addition, IOSCO noticed that “many of the issues and risks associated with trading crypto-assets – are similar to the issues and risks associated with trading traditional securities or other financial instruments on trading venues”.<sup>44</sup>

BCBS: In March 2019, the BCBS issued a “statement on crypto-assets”<sup>45</sup> which outlines its minimum supervisory expectations for banks that acquire crypto-assets and/or provide related services. Even though according to the Committee, the banks globally have limited exposure to crypto-assets, and their size relative to the global financial system is small, the growth and innovation in crypto-asset markets give them the potential

---

<sup>41</sup> See general: **Government of Canada** - Guide, 2019

<sup>42</sup> See general: **IOSCO** 01/2018

<sup>43</sup> See general: **IOSCO** 02/2019

<sup>44</sup> **IOSCO**, 02/2020, p. 3, p. 6

<sup>45</sup> See general: **BCBS** 03/2019

to be systemically important. The statement highlighted a number of risks for banks, including liquidity risk, credit risk, market risk and money laundering risk. The minimum supervisory expectations included inter alia: Conduct of comprehensive analyses of financial and non-financial risks that crypto-assets present, full integration of a robust risk management framework for crypto-assets into the overall bank's risk management process, incorporation of risk assessment into the internal capital and liquidity adequacy assessment processes and public disclosure of material crypto-asset exposures.

Subsequently, in December 2019, BCBS published a discussion paper related to the prudential treatment of “high-risk” crypto-assets<sup>46</sup>, where provided, inter alia, an illustrative example of potential capital and liquidity treatment for banks' direct and indirect exposures (e.g., derivatives) to high-risk crypto-assets<sup>47</sup>. In the same context, the Committee set out three principles a) ‘same risk, same activity, same treatment’, b) simplicity and c) minimum standards<sup>48</sup>. The first principle reflects that the financial risks that banks may face from crypto-assets holdings are not unlike other asset classes and they can be treated in a similar manner. According to the simplicity principle, prudential requirements should be simple and flexible, in order to cover effectively the case that some types of crypto-assets become systemically important. Lastly, BCBS specified that prudential treatment for crypto-assets constitute a minimum standard upon which individual jurisdictions would be free to apply more conservative measures if warranted, including prohibiting exposures.

FSB: The FSB in its May 2019 report on “work underway to address crypto-asset risks”<sup>49</sup> summarized recent work conducted by international organizations and covered a wide range of issues, including investor protection, market integrity, anti-money laundering, bank exposures and financial stability monitoring. The report notes that gaps may arise in cases where crypto-assets are outside the perimeter of market regulators and payment system oversight. The report, which was delivered to G20 Finance Ministers and Central Bank Governors, concluded with a recommendation that the G20 keep the topic of regulatory approaches and potential gaps, including the question of whether more coordination is needed, under review.

Following that, in June 2019, FSB published the report<sup>50</sup> “Decentralised financial technologies”, which considered the financial stability and

---

<sup>46</sup> See general: **BCBS** 12/2019

<sup>47</sup> Ibid, p. 11, 12

<sup>48</sup> Ibid, p. 8

<sup>49</sup> See general: **FSB**, 05/2019

<sup>50</sup> See general **FSB**, 06/2019

regulatory gaps and implications of the use of decentralized financial technologies, such as those involving distributed ledgers and online peer-to-peer or user-matching platforms. The report suggested that the use of decentralized technologies may entail risks to financial stability, including the emergence of concentrations in the ownership and operation of key infrastructure and technology as well as a possible greater degree of procyclicality in decentralized risk-taking<sup>51</sup>.

Moreover, in April 2019, the FSB published “Crypto-assets regulators directory”<sup>52</sup>. The purpose of this directory, which the FSB delivered to the April 2019 G20 Finance Ministers and Central Bank Governors meeting, was to provide information on the relevant regulators and other authorities in FSB jurisdictions and standard-setting bodies who are dealing with crypto-assets issues.

### 3.4 Anti-money Laundering: FATF Recommendations

The Financial Action Task Force (FATF), the international standard-setter for Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF), was the only policy-making body that actually issued standards regarding the application of the AML/CTF existing standards to cryptocurrencies transactions. In its Recommendations<sup>53</sup>, published in 2012 and lastly updated in October 2020, FATF focuses on the significance of the regulation concerning the intermediaries of crypto transactions. In particular, the countries must ensure that “virtual asset<sup>54</sup> service providers are regulated for AML/CTF purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations”. Moreover, the services providers should be required to identify, assess and act effectively in order to mitigate money laundering and terrorist financing risks, in the provision of their services.

While the FATF’s Recommendations are not binding, per se, failure to comply with them may result in severe economic consequences, as the financial institutions in “non-cooperative countries or territories” are spotlighted as suspect. Consequences of non-cooperation may include political condemnation, international investigation, prosecution and sanctions.

---

<sup>51</sup> Ibid, p. 1

<sup>52</sup> See general: **FSB**, 04/2019

<sup>53</sup> See general: **FATF**, 2012-2020 Recommendations

<sup>54</sup> Ibid, p. 17, p. 76: **FATF**, defines a virtual asset as “a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.” This definition is broad enough to also cover crypto-assets.

## Section B. European Union approaches

### 3.5 ESMA's role and primary European law

European Securities and Markets Authority (ESMA), after the explosion of ICOs in 2017, published a Statement<sup>55</sup> and warned investors that ICOs are “*extremely risky*” and characterized them as “*highly speculative investments*”. The Authority highlighted the lack of investors’ protection as a result of the unclear regulatory framework. It also pointed out specific risks around ICOs, such as risks that derive from the high price volatility of coins and tokens, as well as from information asymmetry between the issuers and the investors. Moreover, according to ESMA, uncertainty surrounding crypto-assets also obstructs the development of a sustainable ecosystem.<sup>56</sup>

Currently, and until the new draft Regulation of the European Commission on crypto-assets is adopted and comes into force, there is no widely accepted definition of crypto-assets in the primary EU legislation. During the summer of 2018, ESMA conducted a survey<sup>57</sup> addressed to the National Competent Authorities (NCAs) of the State Members, in which they were asked to indicate whether a sample of six crypto-assets could be legally qualified as MiFID 2 financial instruments. The unclear concepts regarding crypto-assets led to various views and interpretations and therefore the need for the existing legislation to change arose again.

Considering the main characteristics of crypto-assets as described above<sup>58</sup>, the principal question regarding their treatment under EU existing regulation is whether crypto-assets constitute a “financial instrument”, under Directive 2014/65/EU (“MiFID 2”)<sup>59</sup>, “electronic money” under Directive 2009/110/EC (“EMD 2”)<sup>60</sup> or none of the foregoing. “*Financial instruments*” are defined in Article 4(1)(15) of MiFID 2, as are inter alia ‘*transferable securities*’, ‘*money market instruments*’, ‘*units in collective investment undertakings*’ and various derivative instruments. “*Electronic money*” is defined in EMD 2 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 [PSD 2]<sup>61</sup>, and*

---

<sup>55</sup> See general: ESMA, statement, 2017

<sup>56</sup> ESMA, 01/ 2019, p. 18

<sup>57</sup> See general: ESMA 01/ 2019

<sup>58</sup> Under Chapter 1, Section B

<sup>59</sup> Directive 2014/65/EU (MiFID 2).

<sup>60</sup> Directive 2009/110/EC (E-MD 2).

<sup>61</sup> Directive 2015/2366/EU (PSD 2)

*which is accepted by a natural or legal person other than the electronic money issuer”.*

Both definitions 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. Based on the key elements of crypto-assets, it is much more likely that a crypto-asset will qualify as a financial instrument than that it will qualify as electronic money. Nevertheless, each State Member could give its own interpretation, and this could lead to legal uncertainty and to regulatory arbitrage between jurisdictions. The common view on the legal qualification of crypto-assets, when adopted in accordance with the new Regulation for crypto-assets markets, will probably address these issues.

### 3.6 Anti-money Laundering: crypto-assets under AMLD 5

The 5th Anti Money Laundering Directive (AMLD 5<sup>62</sup>) marks the first time in EU history that the use of cryptocurrencies falls under the scope of AML regulation. Money laundering risks derived from cryptocurrencies have been addressed by the EU legislator, mainly by including in the definition of “obliged entities” the so-called “custodian wallet providers” and “providers engaged in exchange services between virtual currencies and fiat currencies”. Within the scope of AMLD 5, these entities should, inter alia, apply due diligence requirements to the customer when entering into a business relationship with them and report any suspicious activity. Certain provisions of the AMLD 5 explicitly address the aspects of virtual currencies. In particular, recital 8 explains the ratio for the directive, noting that, at present, providers of exchange services between virtual and fiat currencies are not subject to the Union's obligation to detect suspicious activity, which in turn facilitates terrorist groups to transfer money to the Union financial system or to virtual currency networks. This legal gap, according to the Directive, makes it necessary to extend its scope to include virtual currencies and e-wallet service providers.

The AMLD 5 has also implications for users (and investors) of cryptocurrencies. Since most users acquire cryptocurrencies through exchange platforms or use the services of wallet service providers in their payments, they will now need to verify their identity with these service providers. Hence, creating a central database that includes all users of cryptocurrencies significantly reduces the sense of anonymity that users now have and, therefore, the risks that this anonymity can cause to the financial system.

---

<sup>62</sup> Directive 2018/843/EU (AMLD 5)

Notwithstanding, in May 2020, the European Commission presented its action plan to strengthen the fight against terrorist financing, where explicitly acknowledged that “*Work at international level suggests a need to expand the scope of sectors or entities covered by AML/CTF rules and to assess how they should apply to virtual assets service providers not covered so far*”<sup>63</sup> and suggested AML innovative technological measures such as the use of remote customer identification and verification as well as the introduction of a ceiling for large cash payments. This acknowledgement has been probably the result of the continuously evolving space of crypto-assets. Since the adoption of AMLD 5, new crypto products and new players, such as wallet custodians, have emerged in the crypto market. As abovementioned, in response to these new developments, the FATF adopted changes to its Recommendations in October 2018 and this leaves behind the EU AML regulatory framework. In order to keep up with the new facts of the crypto market and the international standards, EU regulators should maybe update the anti-money laundering regime. For instance, a broader definition of obliged entities could be adopted, to include trading platforms exchanging crypto into crypto and issuers of crypto-assets. It would also be critical to include tokens in the definition of virtual currencies.

### Section C. New legislation proposal: EU Regulation for Markets in Crypto-assets

On September 24, 2020, the European Commission published its highly-anticipated Digital Finance Package, including legislative proposals and non-legislative communications. One of the legislative proposals published included a draft Regulation on “**Markets in Crypto-Assets**” (**MiCA**) which, as claimed by the Commission, “*will support innovation while protecting consumers and the integrity of cryptocurrency exchanges*”<sup>64</sup>. MiCA, which likely will not enter into force until 2023, applies to crypto-assets not covered by existing EU financial services legislation (e.g., MiFID 2, E-MD 2, PSD 2) and it will be directly applicable to all Member States. It is the first European-level legislative initiative aiming to introduce a harmonized and comprehensive framework for the issuance, application and provision of services in crypto-assets. Once formally adopted, the set of rules provided in the draft Regulation will shape the conduct of business in European markets of crypto transactions.

---

<sup>63</sup> European Commission, 05/2020, p.6

<sup>64</sup> See: <https://ec.europa.eu/digital-single-market/en/legal-and-regulatory-framework-blockchain>

Some of the MiCA Regulation's key provisions are presented in brief just below.

### 3.7 Definitions under the MiCA Regulation

As already mentioned,<sup>65</sup> despite the frequent use of the term, there is no generally-accepted definition of what constitutes a crypto-asset. This is due to the evolving nature of crypto-assets, which also results in the continuous emergence of new crypto-related products and services. MiCA, except crypto-assets, also defines “asset-referenced token” as a *type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets*; This definition includes but is not limited to stablecoins. The provisions about asset-referenced tokens could apply to every kind of asset-backed cryptocurrency, already existed or likely to emerge in the future. Likewise, the term “electronic money token or e-money token” means “*a type of crypto-asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender*”. With this definition, all types of cryptocurrencies that may be used as a means of payment fall under the scope of the new specialized rules and are unambiguously distinguished from the “E-MD 2” term “e-money”.

The new Regulation's definitions will eventually constitute a legislative benchmark. Considering also that when adopted, MiCA is going to be directly applicable to all Member States, it undoubtedly will coordinate the treatment of crypto-assets and facilitate the implementation of rules relating to crypto-assets from the competent authorities, at least within the EU.

### 3.8 Provisions concerning crypto-assets service providers:

In order to ensure the orderly function of crypto-asset markets and limit the risks originating from the anonymity of their users/investors, the new framework contains comprehensive regulation for the most monitorable players of crypto-markets, i.e., the service providers operating crypto-trading platforms.

**(a) Authorisation provisions:** Pursuant to articles 53-58 of MiCA, only legal persons that have a registered office in one of the European EU Member States and have obtained an authorisation from the relevant national competent authorities as crypto-asset service providers, in

---

<sup>65</sup> See above, under 1.7



accordance with MiCA, will be permitted to provide services in crypto-assets. An authorisation in one Member State will be valid for the entire EU, in accordance with a “passport” mechanism familiar from other pieces of European markets legislation. All authorised crypto-asset service providers will be listed on a central register that will be maintained by the European Securities and Markets Authority (ESMA). Thus, MiCA does not provide for a separate third-country regime, meaning that persons located in a non-EU jurisdiction and intending to provide their services to clients in the EU will have to comply with all requirements and obtain full authorisation<sup>66</sup>.

**(b) Other obligations and prudential requirements:** Crypto-asset service providers will be obliged to act honestly, fairly and professionally in accordance with the best interests of their existing and prospective clients. This will include making their pricing policies available for the public, having a transparent fee structure for the services provided to avoid the placing of orders that could contribute to market abuse or disorderly trading conditions, and also have insurance policies covering their clients. In addition, MiCA contains prudential requirements for crypto-asset service providers and in particular, prudential safeguards equal to the amounts specified in article 60 (2). As concerns the insurance policies, the new provisions are very explicit about the types of risks they must cover, which will include loss of documents, acts, errors or omissions resulting in a breach of the duty to act honestly, fairly and professionally towards clients, as well as losses arising from business disruption or system failures<sup>67</sup>.

**(c) Operation of trading platforms:** Persons authorised to provide trading platforms for crypto-assets will have to adopt operating rules for the platform, such as rules for due diligence and approval processes that are applied before admitting crypto-assets to the platform and conditions under which trading of crypto-assets can be suspended<sup>68</sup>. Moreover, they will not be able to deal on their own account on the trading platform they operate<sup>69</sup>. They will also need to put in place effective systems, procedures and arrangements to ensure operational resilience of their trading systems, in order to mitigate operational risks e.g., internet disruptions. These provisions seem to enhance significantly the protection of crypto-assets investors from the risks associated with technical issues of trading platforms and online custodians.

---

<sup>66</sup> MiCA, Art. 58

<sup>67</sup> Art. 60 (5)

<sup>68</sup> Art. 68 (1)

<sup>69</sup> Art. 68 (3)

Finally, the service providers will be subject to MiFID-like pre- and post-trade transparency provisions and will have to ensure that their fee structures are transparent, fair and non-discriminatory<sup>70</sup>.

### 3.9 Provisions concerning the issuance and exchange of crypto-assets

**(a) Issuers of crypto-assets:** MiCA defines a crypto-asset issuer broadly in order to cover as many cases of crypto-offers as possible: issuer is considered any “*legal person who offers to the public any type of crypto-assets or seeks the admission of such crypto-assets to a trading platform for crypto-asset*”. According to article 13, the issuers of crypto-assets will have to comply with some general requirements, such as acting honestly and professionally, communicating with the holders of crypto-assets in a fair, clear, and not misleading manner and managing possible interest conflicts. Issuers of asset-referenced tokens and e-money tokens are subject to more stringent requirements.

**(b) Whitepaper obligation:** It is a shared opinion that tokens offered to investors in ICOs can, in some situations, resemble shares or bonds and they indeed present a financial risk that entails the need to mitigate information asymmetry. The obligation for issuers of crypto-assets offerings to publish a “whitepaper” with mandatory disclosure requirements, laid down in article 7 of MiCA, strengthens this opinion. The white paper seems to have a similar purpose to that of prospectuses in enabling investors to make informed decisions.

More specifically, the issuer of the tokens must notify the whitepaper to the national competent authority at least 20 days before it is published. The issuer is also obliged to provide the competent authority with an “assessment” explaining why the offered crypto-asset does not represent a financial instrument, electronic money, deposit or structured deposit under EU law. The competent authority has the power to require the issuer to amend or supplement the whitepaper or even suspend or prohibit the offering.

Exemptions from these requirements apply and to some extent, they mirror exemptions under the Prospectus Regulation<sup>71</sup> (e.g. if crypto-assets are offered only to qualified investors or less than 150 investors per Member State). However, crypto-assets that are automatically created through mining as a reward for the maintenance of the DLT or the validation of transactions are exempted.

---

<sup>70</sup> Art. 68 (9)

<sup>71</sup> Regulation 2017/1129/EU

Overall, this innovative new legislation describes the most extensive regulation of digital assets to date, capturing the entire gamut of crypto-assets and provides differentiated and detailed rules for the most popular cryptocurrencies, like Bitcoin and Ethereum, for stablecoins like Facebook's digital currency (Libra) and Tether, as well as for utility tokens.

MiCA may have a significant effect on the crypto-asset market. It is possible that crypto-assets covered by MiCA will be viewed as safer investments and, therefore, European crypto-asset markets will be more appealing, possibly to the detriment of other markets, including the UK market<sup>72</sup>. Furthermore, comprehensive regulation will lend credibility to crypto-assets and this may drive banks and other established financial institutions closer to crypto-asset space.

---

<sup>72</sup> In view of Brexit, it is almost certain that the UK will not directly implement MiCA Regulation.

## **Conclusions**

Indubitably, the financial sector is currently undergoing a major transformation. Cryptocurrencies have “escaped” the dark side of the finance universe and have become a discussion and study topic within the investment management industry. Despite crypto-assets having no intrinsic value and being prone to significant price fluctuations, their market share in the world of investments continues to grow. Cryptocurrencies have unleashed a wave of financial innovations, putting competitive pressure on the capital markets and especially with regards to the facilitation of cross-border transfers.

However, their unique cryptographic nature along with their volatile prices, introduce financial risks for their investors. In parallel, the lack of a generally-accepted legal definition of these assets and their hybrid nature have been a barrier to their qualification as traditional financial instruments. Hence, the existing investor protection provisions in most jurisdictions comprise an inadequate regime to mitigate these risks considering the wait-and-see approach by regulatory authorities.

Other key characteristics of crypto-assets, such as their transferability, anonymity as well as their completely digital nature, makes them particularly suitable for money laundering and other criminal activities. This problem has been addressed by EU regulators, with the amendments and the special provisions concerning money laundering risks from cryptocurrencies, included in the 5th AML Directive. However, the rapidly evolving nature of the crypto-asset market, the development of new crypto-assets and advancements in the underlying technology, require legislators to update the legal framework regularly in order to ensure compliance with anti-money laundering requirements within the crypto-space.

Moreover, the risks deriving from crypto trading within the financial system are sui generis and mainly of technical nature. Financial monitoring bodies have supported that the somewhat limited exposures of financial institutions to crypto-assets are not significant enough to jeopardize the system’s stability. Thus, the continuous growth of the crypto-assets market may change this and therefore, supervisory authorities and regulators should remain cautious.

In general, regulators and standards-setters in Europe and around the world, should continue to monitor closely this digital and innovative market and equally adopt innovative rules and procedures. The harmonization of rules and the cooperation among the policymakers, in order to avoid regulatory arbitrage, is pivotal. The European Commission

Proposal for Regulation on markets in crypto-assets comprises a notable example of a set of rules that covers a wide range of existing issues and risks derived from crypto investments. In essence, the new legal framework seeks to streamline the crypto industry and make it investor-friendly. If passed, the MiCA Regulation may transform the European Union into the largest and most significant regulated space for cryptocurrencies globally. Consumers and cryptocurrency exchanges should operate under a clear regulatory framework, the establishment of which, would ultimately enhance market integrity and drive consumer adoption of cryptocurrencies.

As Valdis Dombrovskis, European Commission Executive Vice-President put it, “*The future of finance is digital*”<sup>73</sup>. There can be no assurance that this future will lead to an expansion or a decline of crypto-assets. Thus, if crypto-assets are indeed here to stay, their indigenous digital nature requires a continuous assessment of risks and re-evaluation of regulatory approaches.

.

---

<sup>73</sup> Press remarks on the day of the adoption of the new Digital Finance Package by the European Commission.

## Appendix

### Regulation

**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 with EEA relevance.

**Proposal for a Regulation** Of The European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937

**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

**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”

**Directive (EU) 2015/2366** 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, 23.12.2015, pp. 35-127)

**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

### Bibliography – Sources

#### B

**Basel Committee on Banking Supervision**, 03/2019, “Statement on crypto-assets”, (electronically available via [https://www.bis.org/publ/bcbs\\_nl21.htm](https://www.bis.org/publ/bcbs_nl21.htm))

**Basel Committee on Banking Supervision**, 12/2019 “Designing a prudential treatment for crypto-assets”, December 2019, 11 (electronically available via <https://www.bis.org/bcbs/publ/d490.pdf> )

**Bratspies, Rebecca**, 03/2018 "Cryptocurrencies and the Myth of the Trustless Transaction" (electronically available via <https://ssrn.com/abstract=3141605> )

**Bullmann, Dirk, Klemm Jonas and Pinna, Andrea** (2019), “In search for stability in crypto-assets: are stablecoins the solution?”, ECB Occasional Paper No.230, August 2019, (electronically available via <https://www.ecb.europa.eu/ecb.en.pdf> )

#### C

**Canada’s Government** "Guide for cryptocurrency users and tax professionals." , 03/2020

(electronically available via <https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html> )

**Commodity Futures Trading Commission U.S.A.** 10/2019 (electronically available via <https://www.CFTC.gov/PressRoom/SpeechesTestimony/CTFcfincensecjointstatement101119> )

**Committee on Payments and Market Infrastructure** “Investigating the impact of global stablecoins” <https://www.bis.org/cpmi/publ/d187.pdf>

**Cuervo, Christina, Morozova Anastasiia, Sugimoto Nobuyasu - International Monetary Fund,** Regulation of Crypto Assets; Fintech Note 12/2019 (electronically available via [file:///Users/mariapetraki/Downloads/FTNEA2019003%20\(1\).pdf](file:///Users/mariapetraki/Downloads/FTNEA2019003%20(1).pdf) )

## E

**European Banking Authority**, 01/2019, “Report with advice for the European Commission on crypto-assets”, (electronically available via <https://eba.europa.eu/eba-reports-on-cryptoassets> .)

**European Central Bank**, 12/2019, “Innovation and its impact on the European retail payment landscape”, (electronically available via <https://www.ecb.europa.eu/pub/pdf/other/ecb.other191204~f6a84c14a7.en.pdf> )

**European Central Bank**, 09/2018, Letter from the ECB President to Mr Jonás Fernández, MEP, on a central bank digital currency (electronically available via [https://www.ecb.europa.eu/pub/pdf/other/ecb.mepletter180914\\_Fernandez.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb.mepletter180914_Fernandez.en.pdf) )

**European Central Bank**, 10/2020, “Report on a digital euro” (electronically available via [https://www.ecb.europa.eu/pub/pdf/other/Report\\_on\\_a\\_digital\\_euro~4d7268b458.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf))

**European Commission**, 05/2020, Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (electronically available via [-anti-money-laundering-terrorist-financing-action-plan\\_en.pdf](#))

**European Securities and Markets Authority**, 11/2017, Statement- “ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs) (electronically available via [https://www.esma.ico\\_statement\\_investors.pdf](https://www.esma.ico_statement_investors.pdf))

**European Securities and Markets Authority**, 01/2019 Advice “Initial Coin Offerings and Crypto-Assets” (electronically available via [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391\\_crypto\\_advice.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf) )

**European Securities and Markets Authority** “Annex 1: Legal qualification of crypto-assets – survey to NCAs”, January 2019, (electronically available via [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384\\_annex.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf) )

## F

**Fernandez, Jonas**, 05/2018, Question to the ECB (electronically available via <https://www.europarl.europa.eu/EN.pdf?redirect>)

**Financial Action Task Force**, “Draft Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers” Guidance, 2019 [FATF Recommendations] (electronically available via: <https://static.coindesk.com/wp-content/uploads/2019/06/Embargo-Virtual-Asset-Guidance.pdf> )

**Financial Stability Board** 06/2019 “Decentralised financial technologies Report on financial stability, regulatory and governance implications, (electronically available via <https://www.fsb.org/wp-content/uploads/P060619.pdf> )

**Financial Stability Board** 05/2019, “Crypto-assets: work underway, regulatory approaches and potential gaps”, (electronically available via <https://www.fsb.org/wp-content/uploads/P310519.pdf>)

**Financial Stability Board** 04/2019, “Crypto-assets regulators directory”, (electronically available via <https://www.fsb.org/wp-content/uploads/P050419.pdf> )

**Frankenfield**, Investopedia 2019, definition (electronically available via <https://www.investopedia.com/terms/s/smart-contracts.asp> )

## G

**Gartz, Madeleine and Linderbrandt, Ida** 2018, “Are Cryptocurrencies the Future of Money?”(electronically available via <https://kth.diva-portal.org/smash/get/diva2:1119782/FULLTEXT01.pdf> )

## H

**Prof. Dr. HOUBEN, Robby and SNYERS, Alexander**, 07/2018 Directorate-General for Internal Policies, Study Requested by the TAX3 committee, European Parliament, “Cryptocurrencies and blockchain Legal context and implications for financial crime, money laundering and tax evasion” (electronically available via [https://www.europarl.europa.eu/cmsdata/Study\\_on\\_cryptocurrencies\\_and\\_blockchain.pdf](https://www.europarl.europa.eu/cmsdata/Study_on_cryptocurrencies_and_blockchain.pdf) )

## I

**International Organizations of Securities Commissions**, 01/2019 Board communication on concerns related to initial coin offerings (ICOs),(electronically available via <https://www.iosco.org/news/pdf/IOSCONEWS485.pdf> )

**International Organizations of Securities Commissions** 05/2019, “Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms Consultation Report” (electronically available via <https://www.iosco.org/library/> )

**International Organizations of Securities Commissions** 02/2020 “Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms Final Report” <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf>

**International Monetary Fund**, 2018 “Treatment of Crypto Assets in Macroeconomic Statistics” (electronically available via <https://www.imf.org/ft/2019/pdf/Clarification0422.pdf> )

## L

**Liepajsv, 10/2020 Investing Haven Crypto** (electronically available via <http://liepajsv.lv/zolijas/investing-haven-263.php>)

## M

**Monetary Authority of Singapore**, 12/2017, media release (electronically available via <https://www.mas.gov.sg/news/media-releases/2017/mas-cautions-against-investments-in-cryptocurrencies>)

## N

**Nakamoto, Satoshi** (2008) "[Bitcoin: A Peer-to-Peer Electronic Cash System](https://bitcoin.org/en/bitcoin-paper)" (bitcoin.org 2008)

**New York State Department of Financial Services**, 02/2018, Guidance on Prevention of Market Manipulation and Other Wrongful Activity (electronically available via <https://www.dfs.ny.gov/system/files/documents/2020/03/il180207.pdf> )

## O

**Official Monetary and Financial Institutions Forum & IBM** (2019), Retail CBDCs The next payments frontier (electronically available via <https://www.omfif.org/The-next-payments-frontier.pdf>)



## W

**World Bank**, 2017 Global Findex database- Measuring Financial Inclusion and the Fintech Revolution (electronically available via <https://globalfindex.worldbank.org/> )

## Y

**Yermack**, 2013. Is Bitcoin a real currency? An economic appraisal, Working Paper. (electronically available via [https://www.nber.org/system/files/working\\_papers/w19747/w19747.pdf](https://www.nber.org/system/files/working_papers/w19747/w19747.pdf) )

## Websites:

BitGear <https://www.bitgear.com.au/>

Coinlore-[https://www.coinlore.com/all\\_coins](https://www.coinlore.com/all_coins)

Coingecko <https://www.coingecko.com/en/stablecoins>

## **ΔΗΛΩΣΗ ΠΕΡΙ ΜΗ ΠΡΟΣΒΟΛΗΣ ΔΙΚΑΙΩΜΑΤΩΝ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ**

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία, την οποία υποβάλλω, δεν περιλαμβάνει στοιχεία προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας σύμφωνα με τους ακόλουθους όρους τους οποίους διάβασα και αποδέχομαι:

1. Η διπλωματική εργασία πρέπει να αποτελεί έργο του υποβάλλοντος αυτήν υποψήφιου διπλωματούχου.
2. Η αντιγραφή ή η παράφραση έργου τρίτου προσώπου αποτελεί προσβολή δικαιώματος πνευματικής ιδιοκτησίας και συνιστά σοβαρό αδίκημα, ισοδύναμο σε βαρύτητα με την αντιγραφή κατά τη διάρκεια της εξέτασης. Στο αδίκημα αυτό περιλαμβάνεται τόσο η προσβολή δικαιώματος πνευματικής ιδιοκτησίας άλλου υποψήφιου διπλωματούχου όσο και η αντιγραφή από δημοσιευμένες πηγές, όπως βιβλία, εισηγήσεις ή επιστημονικά άρθρα. Το υλικό που συνιστά αντικείμενο λογοκλοπής μπορεί να προέρχεται από οποιαδήποτε πηγή. Η αντιγραφή ή χρήση υλικού προερχόμενου από το διαδίκτυο ή από ηλεκτρονική εγκυκλοπαίδεια επιφέρει τις ίδιες δυσμενείς έννομες συνέπειες με τη χρήση υλικού προερχόμενου από τυπωμένη πηγή ή βάση δεδομένων.
3. Η χρήση αποσπασμάτων από το έργο τρίτων είναι αποδεκτή εφόσον, αναφέρεται η πηγή του σχετικού αποσπάσματος. Σε περίπτωση επί λέξει μεταφοράς αποσπάσματος από το έργο άλλου, η χρήση εισαγωγικών ή σχετικής υποσημείωσης είναι απαραίτητη, ούτως ώστε η πηγή του αποσπάσματος να αναγνωρίζεται.
4. Η παράφραση κειμένου, αποτελεί προσβολή δικαιώματος πνευματικής ιδιοκτησίας.
5. Οι πηγές των αποσπασμάτων που χρησιμοποιούνται θα πρέπει να καταγράφονται πλήρως σε πίνακα βιβλιογραφίας στο τέλος της διπλωματικής εργασίας .
6. Η προσβολή δικαιωμάτων πνευματικής ιδιοκτησίας επισύρει την επιβολή κυρώσεων. Για την επιβολή των ενδεδειγμένων κυρώσεων, τα αρμόδια όργανα της Σχολής θα λαμβάνουν υπόψη παράγοντες όπως το εύρος και το μέγεθος του τμήματος της διπλωματικής εργασίας που συνιστά προσβολή δικαιωμάτων πνευματικής ιδιοκτησίας. Οι κυρώσεις θα επιβάλλονται, ύστερα από γνώμη της τριμελούς εξεταστικής επιτροπής με απόφαση της Συνέλευσης της Σχολής, και μπορούν να συνίστανται στον μηδενισμό της διπλωματικής εργασίας (με ή χωρίς δυνατότητα επανυποβολής), τη διαγραφή από τα Μητρώα των μεταπτυχιακών φοιτητών , καθώς και την επιβολή πειθαρχικών ποινών, όπως η αναστολή της φοιτητικής ιδιότητας του υποψήφιου διπλωματούχου.

Επιπλέον, παρέχω τη συναίνεσή μου, ώστε ένα ηλεκτρονικό αντίγραφο της διπλωματικής εργασίας μου να υποβληθεί σε ηλεκτρονικό έλεγχο για τον εντοπισμό τυχόν στοιχείων προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας.

**Ημερομηνία**

30.11.2020

**Υπογραφή Υποψηφίου**

