Ca' Foscari
University
of Venice

Master's Degree
in
Economics and Finance

Final Thesis

The EU Commission's Proposal for a Markets in Crypto-Assets Regulation (MiCAr)

Is the MiCAr sufficient to fully regulate the crypto-assets landscape?

Supervisor
Ch. Prof. Andrea Minto

Graduand
Giovanni Bortolato
Matriculation Number 861557

Academic Year
2021 / 2022

TABLE OF CONTENTS

CHAPTER III

BRIEF INTRODUCTORY OVERVIEW

On the 24 of September of 2020, the European Commission took a wider approach to the future development of European digital finance[1] and adopted a new *Digital Finance Package*[2], a group of regulations in which is included the *Digital Finance Strategy*. This new Digital Finance Package consists of legislative proposals on crypto-assets and digital resilience, aiming to improve the competitiveness of EU's financial sector by giving consumers access to innovative financial products, and at the same time by ensuring consumer protection and financial stability.

In particular, the *Digital Finance Package* aims primarily at four major points:

1. Reduce the fragmentation of the EU's digital financial market;
2. Regulate the new-born financial technologies, such as DLT, AI and blockchain;
3. Create a European space of financial datas (Open Finance);
4. Be prepared to the financial sector's evolution.

The portion covered by the above introduced *Digital Finance Strategy* brings three proposals of regulation and one directive:

1. Regulation of crypto-assets' market (MiCA regulation);
2. Regulation establishing a pilot regime for market infrastructures based on distributed ledger technology (DLT);
3. Regulation on digital operational resilience for the financial sector (DORA regulation);
4. Directive which improves other directives (including the PSD2).

All the four points are grouped in the digital finance strategy because of their interconnections, but the first 2 points are to be considered two parts of the same topic. In this essay it will be analyzed the impact of those regulations on financial markets, the possible outcomes and critical aspects of a highly complex structure such as crypto-assets' markets.

[1] ZETSCHE, ANNUNZIATA, ARNER and ROSS, (2020), *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy*, European Banking Institute, Working Paper Series 2020/77, electronically available at: http://dx.doi.org/10.2139/ssrn.3725395.

[2] FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION and EUROPEAN COMMISSION, (2020), *Communication on Digital Finance Package*, electronically available at: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

The *Digital Finance Strategy* (DFS), with the above-described measures, will provide a very long-awaited, comprehensive blueprint for future EU's legislation of fintech. This framework will enlarge the regulation of the EU in the digital finance sector, regulation which today is narrow and not adequate to this big phenomenon. Its four elements (three regulations and one directive) will remove the fragmentation of the Digital Single Market, while adapting the existing fintech regulation to the fintech instruments born with the innovation. In addition, this framework will help the spread of this phenomenon, facilitating the usage of datas in financial sectors, lowering the risks and improving the resilience of the entire economic system. The DFS is said to be long-awaited also because of the size of the market which will be implemented in: for example, in 2020 there were over 5,100 crypto-assets for a total value of over 250 billion dollars.

It must be noted that this is a worldwide data, but it is also worth mentioning that geographical restrictions do not apply (or, at least, not so perfectly) to these kinds of instruments. Crypto-asset is one of the most important categories of instruments treated in the DFS, and one of the reasons in defining the DFS long-awaited is that, de-facto, this category was mostly not regulated (unless for a small part falling under the "*financial instrument*" category, regulated by MiFID II[3]). This topic will be treated in detail further in the thesis.

Focusing on the first proposal of regulation in the Digital Finance Strategy, the Market in Crypto-assets Regulation (MiCAR), the scope of this regulation is very easy to understand: MiCAR goal is to regulate the grey area of items not falling into the category of financial instruments (for example, stocks, derivatives, etc.) regulated by the MiFID II[4]. These items (the so-called "*Crypto-assets*") are instruments capable of creating value, but the regulation of financial instruments is not sufficient and, most importantly, not fully able to cope with this complex and heterogenous market. Therefore, the EU decided to finally try to fill this gap (as said before, a large gap worth billions of euros also in the

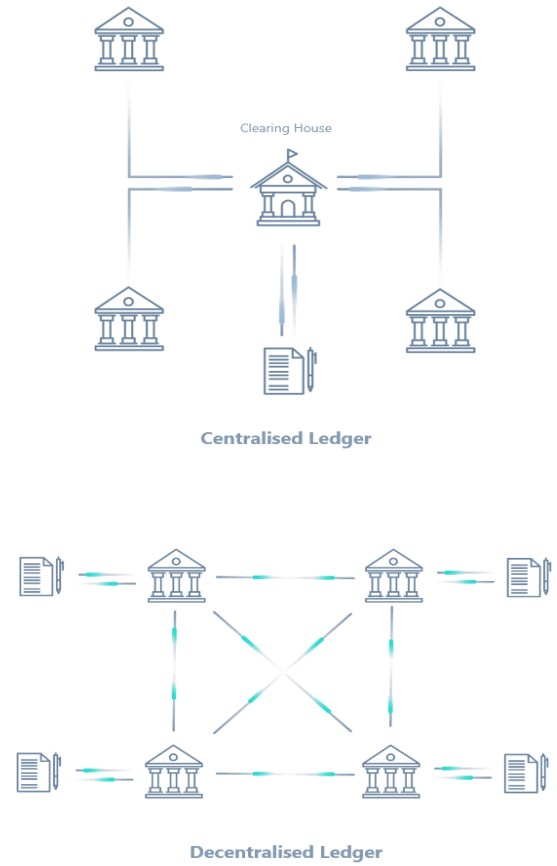
3 MiFID II (2014/65/EU) is the EU directive that replaced the first *Markets in financial instruments directive* or MiFID (2004/39/EC) which stayed in force from 31st January 2007 to 2nd January 2018.
On this matter, LAURENT, *The tokenization of assets is disrupting the financial industry. Are you ready?*, Inside magazine issue 19 – Part 02: from a core transformation/technology perspective, Deloitte, 2018, p. 6 ff.

4 The Directive 2014/65/EU is electronically available at: https://eur-lex.europa.eu/eli/dir/2014/65/oj.

EU) using the MiCAR proposal. The first and most important task to do, however, was to finally define what a crypto-asset; however, as it will be shown in the following chapters, this is not an easy task because of the huge number of differences and purposes of these items. For this particular reason, before analysing in depth the specific features of the EU MiCA regulation and its implications, it might be best to picture the topic from a broader perspective, starting with some definitions first, in order to have a better understanding of what crypto-assets' nature is and why is it so difficult to sufficiently regulate them.

1. DLT

Before going in the details of what a crypto-asset is, it must be defined the underlying technology. As a matter of fact, crypto-assets can be described as digital representations of «a value or right which may be transferred and stored electronically using Distributed Ledger Technology or similar technology»[5].

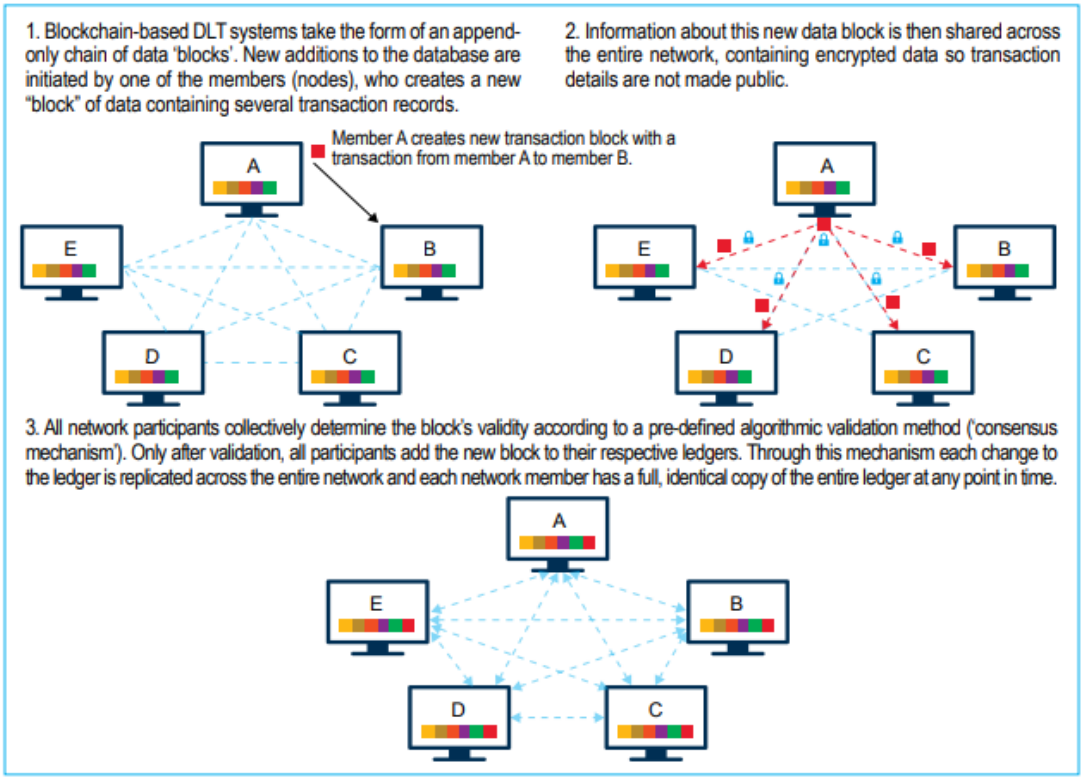


Source: Marco Polo Network, 30 January 2018. Electronically available at: https://marcopolonetwork.com/distributed-ledger-technology/

[5] EUROPEAN COMMISSION, (2020), *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets and amending Directive (EU) 2019/1937 (MiCA)*, electronically available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

The so-called Distributed ledger technology (**DLT**)[6] can be described as a technology in which the information of the usage of that asset are not stored in a central database, instead they are stored among all its users, spreading all over the world (blockchain is a typical example of DLT).

Figure 1: How Does Blockchain-Based DLT Work?



Source: Adapted from: "Dubai Aims to Be a City Built on Blockchain", By Nikhil Lohade, 24 April 2017, Wall Street Journal

To put it short, it is a *protocol* that enables the secure functioning of a decentralized digital database.

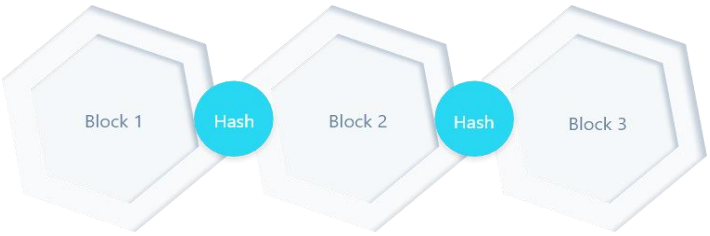
Another key and common aspect is that a crypto-asset (as said before) is not controlled or guaranteed by a public/central authority: distributed networks eliminate the need for a central authority to keep a check against manipulation, In fact, the very nature of a decentralized ledger makes them immune to a cyber-crime, as all the copies stored across the network need to be attacked at the same time for the attack to be successful. Additionally, the simultaneous (*peer-to-peer*) sharing and updating of records on the entire network make the whole process much faster, more effective, and cheaper.

[6] On how to define a DLT: RAUCHS, GLIDDEN, GORDON, PIETERS, RECANATINI, ROSTAND, VAGNEUR and ZHENG, (2018), *Distributed Ledger Technology Systems: A Conceptual Framework*, electronically available at: https://ssrn.com/abstract=3230013 or http://dx.doi.org/10.2139/ssrn.3230013.

It is in fact a common opinion and a proven fact that DLT typically grants several potential advantages over traditional centralized (or other kind of) ledgers, including decentralization and disintermediation, improved transparency and security checks, improvement in executions and efficiency, cost reductions, automation and programmability.

DLT allows for storage of all information in a secure and accurate manner using cryptography. The same can be accessed using "keys" and cryptographic signatures. Once the information is stored, it becomes an immutable database and is governed by the rules of the network. To clarify, DLT are not immune to hacking techniques: theoretically possible, an hacker would need to manipulate simultaneously most of the record of the network, in order to manipulate the data. Theoretically possible as said, but highly unlikely, also considering the dimensions of DLT network. Hackers surely prefers to attack single users, but this will be discussed later in the next chapters.

Having summarized the main characteristics of the DLT technology, it's better and useful to also define the main features of the blockchain technology. The most important difference to remember is that blockchain is just one type of distributed ledger. Although blockchain is a sequence of blocks, distributed ledgers do not require such a chain. In fact, the **blockchain** is essentially a shared database (here it is the DLT framework) filled with entries that must be confirmed and encrypted. A practical example would be comparing the blockchain to the pages of a book: the last page implicit stores information of the previous page, which is itself based on the previous one, and so on. This "chain-like" frame gives the name to the technology: the name blockchain refers to the "blocks" that get added to the chain of transaction records. Going in the technical details, the technology uses cryptographic signatures called "hash", in order to link the different blocks.



Source: Marco Polo Network, 30 January 2018. Electronically available at: https://marcopolonetwork.com/distributed-ledger-technology/

Blockchain-based DLT was first implemented and practically used as the underlying technology of the crypto-currency *Bitcoin*, but it has a variety of potential usages beyond the specific sector of digital currencies/crypto-currencies. In fact in recent years, we've seen that the DLT has possible applications in cross-border payments, financial markets infrastructure and in collateral registries, but not only in financial-related environments: potential usages of DLT are currently being studied and experimented, for example in digital identity products (such as national ID, birth, marriage and death records) or in the industrial sector, improving the supply chain process of the raw materials (for example in automatically checking the quality and the information of the commodities received).

That said, the technology itself is still evolving, besides its applications, and new risks currently without a mitigation may appear. Some areas of risks are IT, legal and regulation compliance: a focal point which must be addressed worldwide is certainly identity verification, data privacy and (usually) anonymity. Developing a legal and regulatory framework for DLT implementations (for example, crypto-assets) is fundamental and necessary, yet not easy at all.
Having briefly described the general technology principles, and the different shapes and application of such innovative technology, we can introduce the already mentioned concept of ***crypto-asset***.

2. Crypto-assets

Moving our geographical scope in Europe, certainly not the mainland of DLT-blockchain-crypto-assets, defining a control framework for such evolving environment was necessary, as one of the main features of such innovations is the absence of geographical restrictions.

The first issue faced by the EU was (and still is) certainly defining what a crypto-asset is. Multiple definitions were released prior to the MiCAr proposal, different points of view highlighting different aspects and characteristics of these items.

In particular:

1. The **ECB Crypto-Assets Task Force** has defined the term very narrowly as «any asset recorded in digital form that is not and does not represent either a financial claim on, or a financial liability of, any natural or legal person, and which does not embody a proprietary right against an entity»[7].

2. **IOSCO (International Organization of Securities Commissions)** has defined the term as «a type of private asset that depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, and can represent an asset such as a currency, commodity or security, or be a derivative on a commodity or security»[8].

3. The **FSB** has put forward a similar definition and defines the term as «a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value»[9]. This definition is also referred to in BIS documentation.

4. In line with the FSB's definition, the **ESMA** has defined a crypto-asset as «a type of private asset that depends primarily on cryptography and DLT or similar technology as part of their perceived or inherent value ESMA uses the term to refer both to so-called 'virtual currencies' and 'digital tokens' (which it defines as "any digital representation of an interest, which may be of value, a right to receive a benefit or perform specified functions or may not have a specified purpose or use"). According to the ESMA, crypto-asset additionally means an asset that is not issued by a central bank[10].

---

[7] RAUCHS, GLIDDEN, GORDON, PIETERS, RECANATINI, ROSTAND, VAGNEUR and ZHENG, (2018), *Distributed Ledger Technology Systems: A Conceptual Framework*, electronically available at: https://ssrn.com/abstract=3230013 or http://dx.doi.org/10.2139/ssrn.3230013.

[8] IOSCO, (2020), *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*, electronically available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf.

[9] HOUBEN and SNYDER, (2020), *Crypto-assets: Key developments, regulatory concerns and responses*, Study PE 648.779, electronically available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf.

[10] *Ibid.*

5. The **EBA** has defined a crypto-asset in a similar way as «an asset that: a) depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, b) is neither issued nor guaranteed by a central bank or public authority, and c) can be used as a means of exchange and/or for investment purposes and/or to access a good or service»[11].

Needlessly to say, it is easy to recognize that all these different organizations (such as ECB crypto-assets task-force, IOSCO, FSB, ESMA and EBA) have found different definitions of what a crypto-asset is, but with some common key aspects; the most common features are two: these different items are all digital assets, and they are based on a **DLT** technology.

Various papers and studies have been made only with the intention of defining the perimeter of crypto-assets, which is the first vital step in initiating the process of regulation. One study in particular released in 2018 by Prof. Dr. Robby Houben and Alexander Snyers, requested by the ECON Committee ("European Parliament Committee on Economic and Monetary Affairs" – European Parliament) addressed the problem.

The abstract is the following:

«*This study, prepared by Policy Department A, sets out recent developments regarding crypto-assets. These relate mainly to the continuing use of crypto-assets for money laundering and terrorist financing, the massive growth of private "tokens" used to raise funds, and to the emergence of stablecoins and central bank digital currencies. The study, furthermore, addresses key regulatory concerns, considering these recent developments, and suggests regulatory responses*». (Houben and Snyers, 2020, p. 75)

As said the problem, especially in 2018, was in defining not only the general definition of crypto-asset to be used, but also in identifying the practical example of such technology. Why? Because of the different shapes of applications of such technology, also considering the fluidity of the entire environment.

As mentioned before, the crypto-assets can take on different forms and have different characteristics (besides the generic ones). The first key division could be made

[11] *Ibid.*

considering the usage of the tool and its function: we can in fact distinguish between crypto-currencies on one side, and tokens on the other:

1. Crypto-currencies (or coins), such as Bitcoin, Litecoin, Dogecoin are a kind of crypto-asset that is designed with the purpose to act as a (digital) currency. The key characteristics are the store of value, a unit of account and the possibility to use them as a payment method. They are designed to act as a peer-to-peer alternative to government-issued legal currencies. They will be the focus of this study, as the regulations of platforms will highly impact crypt-exchanges.

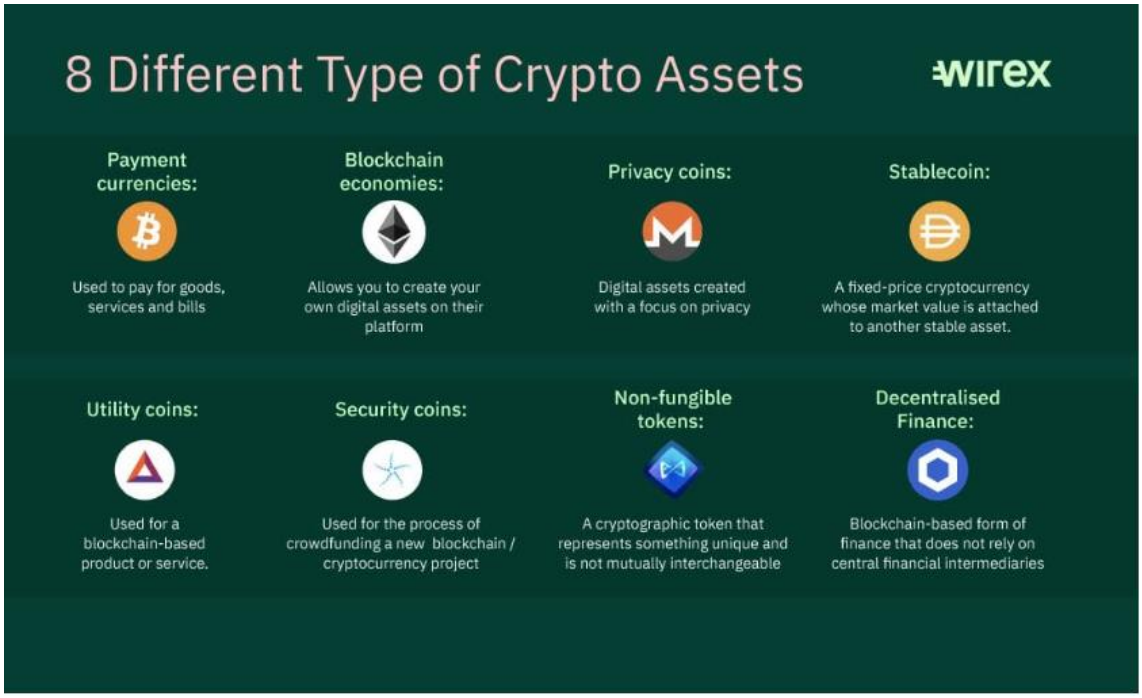
2. Tokens are a kind of crypto-asset with a lot of different shapes, in perspective more than the crypto-currencies counterpart. The general adopted definition in fact is: «*a crypto-asset is considered as a token if it offers their holders certain economic and/or governance and/or utility/consumption rights*»[12]. (Snyers e Houben, 2020, p.18) Such definition is understandably generic. To have a better idea of what can be considered as a digital token, we can describe them as a digital representation of interests, or rights to (access) certain assets, products, or services. Practically, crypto-tokens can be used to represent an investor's stake in the company (stocks) or they can be used for an economic purpose. This means token holders can use them to make purchases (but not mix them with crypto-currencies), they can trade tokens just like other commodities or practically use them. Why are there so different usages? Just like crypto-currencies, also for tokens there is more than one category, depending on the nature and the purpose of the specific item, as tokens can take on different forms with diverse features, more than the crypto-currencies. Generally speaking, in recent years most regulatory authorities and legal scholars worked with the intention to divide tokens into categories: the result is the distinguishment of the so-called *investment* / *security* / *asset tokens* from *utility* ones.

    a. Investment tokens – sometimes also referred to as security tokens or asset tokens – are that category of items that generally provide their holders

[12] On this particular matter, SNYERS and PAUWELS, (2019), *De ITO: a new kid on the block in het kapitaalmarktenrecht*, Larcier, Bruxelles, p. 122 ss., electronically available at: https://hdl.handle.net/10067/1621030151162165141; MASS, (2019), *Initial coin offerings: when are tokens securities in the EU and US?*, p.21-23, electronically available at: https://ssrn.com/abstract=3337514.

rights in the form of ownership similar to dividends. Such sub-category is generally issued through an ICO (Initial Coin Offering) for capital raising purposes. The term “investment tokens” refers to the properties of such items, making them comparable to debt and equity. The sub-category does not contain only this kind of items: the term “investment token” is also used in referring to traditional securities, assets or commodities that have undergone the process of tokenization (for example, a stock that have been digitalized in a form of a token, with a blockchain underlying technology).

b. Utility tokens are the sub-category of tokens that grant their holders access to a specific application, product, or service, often provided through a blockchain-type of infrastructure. The main difference from other types of items (such as crypto-currencies) is that they typically **only provide access to a product or service developed by the issuer,** and they are not meant and accepted as a payment method for other services or products of the same issuer and, of course, of others. They can be seen as an access key, sometimes as an advanced security system, not as a real, tradable asset. They are linked to the investment tokens by the general environment in which they are released: some kind of utility tokens are issued to collect (economic) resources, usually fund. However, unlike investment tokens, their main purpose is not to generate future cash flows for investors (as, for example, tokenized shares), but to grant access.



Source: Wirex, 10 November 2021. Electronically available at: https://wirexapp.com/blog/post/the-8-different-types-of-crypto-assets-0471

Having given a quick overlook of the different shapes of items which can be classified as crypto-assets, it's easy to spot the problem: how can we address the different needs, with a single, common regulation?

Before introducing the various types of regulations, or at least the attempts to do so, it is necessary to introduce the roles of Central Banks and their approach to the crypto-environment. The quick growth in popularity of the cryptocurrencies (but also tokens, from the companies' point of view) and their underlying technology have moved various CBs (Central Banks) to invest a lot of funds in studies, researches and projects with the objective to understand whether it would be reasonable and appropriate for them to issue their own digital currency, for business purposes (just like an investment), or as a clear substitute for physical banknotes and coins in future years. This matter is not fully applicable to the token side, as they are quite different in scope and characteristics, as they are considered more as a utility than an investment.

Returning to the digital currencies studied (and in the future, issued) by central banks, they are commonly referred to as central bank digital currencies (CBDCs). The definition is truly easy and straightforward: "CBDC is a digital asset, or a digitalized instrument issued by a central bank for the purpose of payment and settlement, in either retail or wholesale transactions"[13]. Since it is issued by a central bank, it would be backed by the securities of the CB, and as a result it could be described as a sovereign coin.

The general opinion of various central banking and monetary policy institutions is that issuing a CBDC is not contingent the usage of a specific technology such as DLT, as it would be possible to issue a CBDC without the DLT framework, and so without the blockchain technology.

In reality, the concept of CBDCs is closely linked to the DLT approach, as the explosion of crypto-currencies has attracted a lot of attentions. The possible issue of CBDC (de-facto crypto-currencies officialized by CBs) could have huge and diverse benefits, with a devasting boost to the development of such technology. Yet at the same time, they also raise various concerns, from monetary policy to cybersecurity to regulation requirements.

While crypto-currencies' main (and basic) objective is to perform the roles of currency, CBDCs are digital currencies, with (in part) the same objective and scope. However, the similarities and comparisons won't go much further. As already described, crypto-currencies (a particular category of the crypto-assets group) are private by nature, generally constituted on a DLT framework and are not issued or backed by any legal entity (a company or a central bank): this is the focal difference with CBDCs. We could see them as two ways to achieve (partially) same results.

[13] OMFIF and IBM, (2019), *Retail CBDCs. The next payments frontier*, electronically available at: https://www.omfif.org/wpcontent/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf.

2.1. Introducing the regulations: backed assets vs non-backed assets

Crypto-assets are commonly considered "something with value", more comparable to a real commodity than a simple currency, at least as the market thinks. But there's a focal point to mention: **crypto-assets in general** (and with crypto-currencies in particular understanding the matter is straightforward) **do not represent any underlying asset, claim or liability**, **making them prone to high price volatility**[14]. Why? Simply because the intrinsic value of the crypto-asset does not reflect the value of an underlying commodity/physical asset.

For example, let's consider two cases, stocks of an oil company, and a crypto-currency:

- **Oil company stocks**: of course, the price will be determined on supply-demand principles, but also on availability, political conditions, economic conditions, specific conditions of the company. Price fluctuations will be present, but without a huge volatility.

- **Crypto-currency**: as there's no underlying asset, a part for the technology used and the possible future implementations, the value will be determined largely thanks to the balance between sellers and buyers on the crypto-exchange, with huge price volatility (fluctuations).

This example gives an idea of the difference between a backed asset and a non-backed asset. Crypto-currencies (but often, crypto-asset in general, even if tokens have some exceptions) are "non-backed" securities. As mentioned, the highly volatile price (and so, value) of traditional "non-backed" crypto-currencies make it very difficult for such items to truly act as a currency, substituting its role of payment method, and so limiting their adoptions at least in a short-medium term perspective.

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

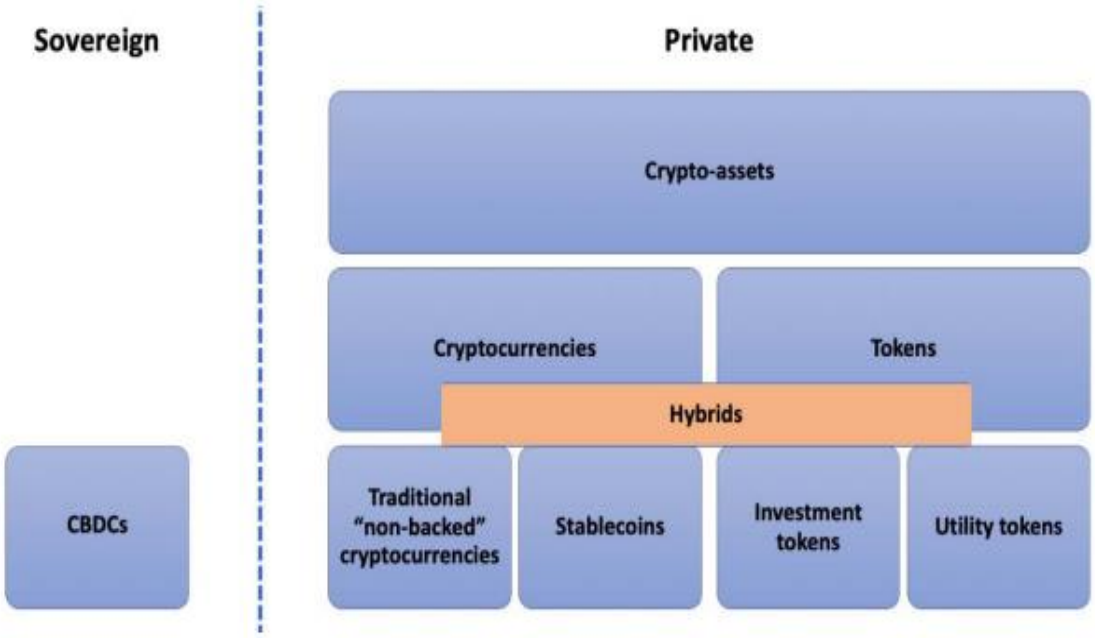
Some crypto-currencies are limited (for example, Bitcoin's limit is 21 million coins) by protocols' restrictions, and experts think this will limit the price fluctuations in the long term, becoming store-of-value commodities, comparable to gold.

Worth mentioning is the concept of stable coins. In an attempt to address the problem of high-volatility, some people started to design crypto-currencies linked to the price of another asset or a pool of assets, designed to maintain a stable value. The so-called Stablecoins are not traditional "non-backed" crypto-currencies, but a subgroup of "backed" cryptocurrencies intended to act as a currency, substituting its role of payment method. The benefit of a (quite) stable price comes with a constraint: unlike traditional "non-backed" crypto-assets, which are generally decentralized with as absence of an identifiable issuer/an institution which grants for the asset's value towards the coin's users, stablecoins typically represent a "right" on a specific issuer/underlying assets/funds. As could be noted, they are a hybrid between "non-backed" crypto-assets, and tokens.

However, whereas tokens are issued with a very specific functionality or for a specific role (e.g., to provide their holders ownership rights and/or dividend-like rights, or to enable access to a specific product or service)[15], stablecoins generally lack such functionality. They are intended to be used as a general-purpose medium of exchange: to enable the buying and selling of a good or service provided by someone other than the issuer. Therefore, they should be distinguished from tokens, rather than be identified as such[16].

Stablecoin's value is, in other words, backed by something with value and not just perceived to be "something of value" itself.

[15] EBA, (2019), *Report with advice for the European Commission on crypto-assets*, electronically available at: https://eba.europa.eu/eba-reports-on-cryptoassets.
[16] HOUBEN and SNYDER, (2020), *op. cit.*



Crypto-assets: Key developments, regulatory concerns and responses. - Prof. Dr. Robby HOUBEN & Alexander SNYERS

CHAPTER I

REGULATORY CONCERNS AND BACKGROUND OF MiCAr

As we have seen in the paragraphs above, the crypto-assets landscape is very heterogeneous, presenting a lot of grey areas.

Before going into details, it is necessary to deepen the various concerns regarding crypto-assets, general concerns (as money-laundering) as well as specific ones (for example, regarding to stablecoins).

Stablecoins were the last type of crypto-asset described in the introduction, because due to their characteristics, their concern is one of the most important and difficult to resolve, and so the first one addressed in various studies. The concern is related to financial stability.

1. Global stablecoins as a threat to financial stability and monetary policy

As described above, the global usage of stablecoins could provide various benefits to the world's financial system (but not only), especially by lowering transaction fees extra-borders operations, evading taxes, embargos, fees and currency changes. This comes with a cost: their global usage also poses new risks and difficulties for financial stability and monetary policy for the competent authorities.

For example, regarding financial stability, various risks can be identified, each different from the other:

- As stablecoins are backed by assets, in a case in which that asset is commonly considered **safe**, an increase of purchases of such underlying asset could cause an increase of the stablecoin price, and therefore a shortage of the coin in certain markets, leading to instability[17];

[17] G7 WORKING GROUP ON STABLECOINS, (2019), *Investigating the impact of global stablecoins*, electronically available at: https://www.bis.org/cpmi/publ/d187.pdf; COUNCIL OF THE EUROPEAN UNION (2019), *Joint Statement by the Council and the Commission on Stablecoins*, electronically

- In a case in which a stablecoin is perceived as a better method to store value than a local fiat currency, common sense would drive citizens to buy a lot of coins and collectively seek for protection during financial turmoil. This would lead to domestic financial instability as during hard times, a big percentage of citizens' net worth would be invested in a currency with no monetary policies and no competent authorities[18];

- Linked to the previous cases, the spread in stablecoins usage could mean a decline in deposits at banks because of the already describes scenarios. This would increase banks' dependence on more costly and volatile sources of funding in order to replace the funds obtained with the deposits, therefore potential financial stability risks could appear, as banks could become underfunded or funded at higher costs[19];

- One of the main concerns regards the credibility and the future of the stablecoins. This concern is related to the previous ones, as this would affect the coin itself: there may be financial stability risks if their credibility gets questioned, as many users would want to opt out, leading to a sell-out crysis. This is a particular problem, as the effects could be devasting: remember in fact that stablecoins are backed by assets, and a shortage of stablecoins could cause serious liquidity problems for banks and institutions that have big reserves of the underlying assets. The effects are not known, but the theoretical studies have shown that the effect could be devasting[20];

available at: https://www.consilium.europa.eu/it/press/press-releases/2019/12/05/joint-statement-by-the-council-and-the-commission-on-stablecoins/.

[18] ZETSCHE, BUCKELY and ARNER, (2019), *Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses*, European Banking Institute Working Paper Series 2019/44, p. 23, electronically available at: https://ssrn.com/abstract=3414401; G7 WORKING GROUP ON STABLECOINS, (2019), *op. cit.*, p. 14.

[19] FINANCIAL STABILITY BOARD, (2019), *Regulatory issues of stablecoins*, electronically available at: https://www.fsb.org/wp-content/uploads/P181019.pdf; G7 WORKING GROUP ON STABLECOINS, (2019), *op. ult. cit.*

[20] *Ibid.*, p. 12 ss.

- Lastly, but probably the biggest concern, it's a scenario in which global stablecoins become well established, with the spread in usage by the public in day-to-day various operations. This would lead to a drift in the ownership of the control of monetary policy from central banks and authorities to private large companies owning a big percentage of the currency, as they would be able to alter and manipulate the market conditions. The big issue with this scenario is that these organizations with no experience on monetary policy, and no general obligation towards users to act in their best interest, would be responsible of the course of a globally used coin[21].

A useful study in this sense was performed in 2019, during the G7 meeting[22]. This preliminary research with an impact analysis of the stablecoins' spread suggests that:

1. It would weaken the effects of monetary policy on local currencies, on interest rates and financing conditions;
2. It would increase cross-border capital mobility (a benefit but also a problem), which would impact the so-called "capital controls", an important measure in monetary policy used to prevent huge capital movements during severe crisis and periods with economic distress, that would enlarge the financial instability.

2. No credible contribution to own funds: Financial institutions with crypto-assets on their balance sheet

Moving from stablecoins' specific case to the larger cryptocurrency category (but also crypto-asset, as some tokens could be considered too), EU financial laws do not prohibit banks, financial institutions, and private companies (including credit institutions, investment firms, payment institutions and e-money institutions), from buying or exposing themselves to crypto-assets or **from offering services relating to crypto-assets**. This line of service is completely permitted, in fact the current limitations only regard the sector of such intermediaries (in the banking sector, for example, a license is requested).

[21] ZETSCHE, BUCKELY and ARNER, (2019), *op. cit.*, p. 23.
[22] G7 WORKING GROUP ON STABLECOINS, (2019), *op. ult. cit.*

Business activities involving crypto-assets (varying from direct investing, advising and exchanging) usually fall in the second category listed above, for the already cleared reason of crypto-assets not being treated as financial instruments, and because (usually) they are not specifically prohibited by national laws. Right now the main concern of financial institutions having crypto-assets in their balance sheet is that the value provided by these instruments to the company is not secure, transparent and straightforward.

The reason behind the balance sheet incorrectly representing the financial situation of companies having crypto-assets in their portfolios is related to the behavior of such instruments. In fact, most crypto-assets:

1. have a really high volatility (this is common also in "non-backed" derivatives, the same rule applies to non-backed crypto-currencies) because their actual value only depends on the combination of demand/offer;
2. are not really resilient in times of financial distress. This is closely related to point 1: when the demand shows signs of slowing down because of a general bad financial situation by the markets, the price immediately falls, generating quick sell-outs.

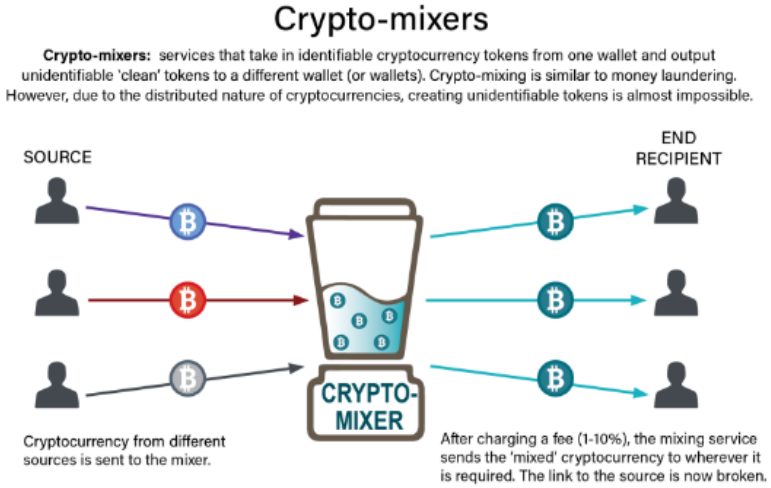
In other words, when the financial institutions insert these instruments in their balance sheet, they are also acquiring a big exposition on huge risks, related to the frenetic changes in the value flow. As a results, besides being a speculation investment, investing in crypto-assets is not always a suitable activities because of the big losses that can occur, and also because it is usually not aligned with the business of the company.

But having financial companies with crypto-assets in their balance sheet is not only a problem of general financial stability, is a problem also in truly representing the value of the company. In fact, consider for example Company A, with problems in successfully creating consistent cash flows. With the remaining funds, the Company buys a reserve of crypto-assets, with the objective of pumping the numbers of the balance sheets, as a result in being more attractive to external investors. The investment goes well, the value of the crypto-assets is raised and they realized a profit: the problem is that the balance sheet shows an improvement, but the core business is still lacking.

The result is a balance sheet representing a distorted picture of the financial situation of. As for industrial companies it is more difficult to hide this distorted picture, because of the differences between crypto-assets and core businesses, for financial institutions (banks, investment firms, etc.) the phenomenon is easier to apply. Therefore, the Supervisory authorities have a central roles in controlling.

3. Concern: money laundering and other illicit usages

After the initial and difficult task of addressing what a crypto-asset is, it must be defined what a crypto-assets is used for. To start with, it must be said that crypto-assets are used for 2 main purposes: legal activities and illegal activities. Most legal activity is concentrated on crypto-exchanges (trading, speculation, etc.) meanwhile illegal activities include buying and selling of illegal goods or services online in dark web marketplaces, terrorism financing, money laundering, evasion of capital controls, payments in ransomware attacks and thefts. Just to note, an Australian study determined how mostly half of all the transactions made with Bitcoin (BTC) were made with illegal purposes. Besides the final illegal acts (tax evasion, money laundering) which are already covered by national laws, the EU's will is to regulate also the instruments used in doing illegal activities exploiting those blind spots in the law.



United Nations, Money laundering through cryptocurrencies, electronically available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html

Talking about money laundering and terrorism financing, the risk is that criminals could exploit. They exploit some common features of the crypto-assets (and more in specific, crypto-currencies): fully digital, easily transferable, pseudonymous– and with the use of specific anonymity-enhancing technology even completely anonymous – assets that operate on a decentralized basis. They have become the perfect financial instrument for illegal purposes. But this phenomenon is not new, at all: well before MiCAr proposal, well before ESMA advice on crypto markets, the TAX3 committee of the European Parliament requested a study, on July 2018, called: "*Cryptocurrencies and blockchain Legal context and implications for financial crime, money laundering and tax evasion*" in which the main illegal purposes of the new crypto technology are described. Again, back in 2018 the main focus was on a particular type of crypto-assets (crypto-currency), but that study remains accurate today, as the crypto-currencies are the most (illegal-purpose) used type of crypto-asset among the others.

As written above, the main feature appreciated by illicit users is anonymity. This is the main concern in preventing illicit money laundering and terrorism financing: the anonymity prevents the transactions (and therefore, the users) from being supervised. This, combined with a not so clear regulation of those items, allows criminal organizations to use crypto-currencies (and more in general, crypto-assets) to obtain clean cash, unlinked to illicit activities.

Regarding terrorism financing, famous was the Ali Shukri Amin case in 2015: he operated a pro-ISIS Twitter account (from Virginia, USA) and a blog and also provided instructions to ISIS supporters on how to use Bitcoin to mask the provision of funds to Daesh in order to avoid currency transfer restrictions. He was arrested in 2015 and sentenced to 6 years in prison. He was released in 2020. Ali surely was quickly arrested for "*Material support to a terrorist organization*", but a surely large and not-known amount of ISIS users managed to transfer money to Daesh, certainly also from EU countries. This phenomenon highlights another key feature in crypto-assets (crypto-currencies in specific): they are not linked to a physical territory/country as there's quite always an absence of a central controlling authority.

Having listed the regulatory concerns and aspects which will be addressed with a proper regulation, it is now necessary to list all the different problems in implementing such regulation.

4. Uncertainty of how existing EU rules will apply to crypto-assets

MiFID II is the central part of EU financial legislation: it clearly defines what a 'financial instrument' is, as well as 'transferable securities'. But MiFID II isn't the only legislation in place for these topics: a broader set of rules are also applied, for example, the MAR, EMIR (European Market Infrastructure Regulation), SFD (settlement Finality Directive). As already mentioned above, when considering how the existing EU financial regulation applies to crypto-assets, the first fundamental task (and issue) is to determine which crypto-assets will be considered as 'financial instrument' under MiFID II, becoming de-facto almost fully regulated by day one.

As already said, the actual crypto-assets landscape is far from homogeneous, and the actual analysis of which crypto-assets will be classified as a financial instrument under MiFID II would require a complex case-by-case approach, with differences between Member States. In fact, the classification could vary, depending on how the definition of 'transferable security' has been interpreted and implemented differently by each Member State. The result is not as straightforward as someone may think: it would be possible in fact that the same crypto-asset could be treated as a "transferable security" (or another financial instrument) in one Member State jurisdiction but not in another. This jurisdictional problem would be particularly hard to solve and to deal with: as already said in previous paragraphs, the crypto-assets nature is global and borders-free, and geographical problems are hardly reflected and represented. Having determined the impossibility to regulate directly the items (as there are no real issuers/central company), the result would be a to market regulation of the users, which would lead to a fragmentation of the EU single market policy[23].

[23] ESMA, (2019), *Report on Licensing of FinTech Business models*, electronically available at: https://www.esma.europa.eu/sites/default/files/library/esma50-164-2430_licensing_of_fintech.pdf. In its report, ESMA states: «Almost all NCAs indicated having difficulty in determining when crypto-assets are regulated and when they are not. NCAs raised the question of the legal nature of the crypto-assets and whether they fit into the definition of MiFID financial instruments, and more specifically, transferable securities».

This possibility is, nowadays, much more realistic than it looks, here's why:

Firstly, the notions of "financial instruments" and "transferable securities" under MiFID II is not harmonized, as demonstrated by ESMA. The fragmentation in the legislation is not an hypothetical situation, but it is, indeed, the reality. EU Member States have not interpreted and implemented the MiFID II in a coherent, unique way: as cited above, ESMA in 2019 has demonstrated that the majority of national competent authorities (NCAs) have not used a specific rationale/criteria (in addition to the **general** parameters set by the EU) in identifying the securities in the scope of national laws for the application of MiFID II. Others NCAs (the minority) do have implemented some specific criteria. It is straightforward to notice the different treatment and implementation
[24].

Secondly, as written multiple times, the crypto-assets are diverse and many of them have hybrid features. The different implementation and treatment by NCAs is not only due to different views of the same items, but also of different views in relation to different aspects of crypto-assets.

For example, let's consider *Token Alpha*.

Token Alpha is a special hybrid token just launched on the EU market, which can be used as a payment method (like a fiat currency) on the main e-commerce sites, but it also remunerates the users by periodically giving them a coupon, like a common bond. The Token Alpha is used all over EU countries. Country A and country B start thinking if and how the token should be regulated under the MiFID II.

A. Country A reasoning is: "the token main purpose is to act as a payment method, and the periodical coupon is not a remuneration of the investment, it can be considered as the value fluctuations of a common fiat value. Therefore, token Alpha is not a financial instrument";

B. Country B reasoning is: "as it is indeed true that the token main feature is to act as a payment method, it's also materially relevant the feature of coupon

[24] All Member States, except Poland. In addition, two EEA Member States (Liechtenstein and Norway). ESMA, (2019), *Annex I – legal qualification of crypto-assets – survey to NCAs*, electronically available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf.

remuneration, as it acts perfectly as a common bond. Therefore, token Alpha has to be considered a financial instrument".

This practical, but very easy example reflects the reality: in this case both NCAs are completely true, as their jurisdiction is in line with MiFID directive. They are simply focusing on two different aspects of the same (complex) item. While some investment tokens could be easily considered as transferable securities or as other financial instruments, payment tokens and utility tokens are more likely to fall outside the scope of the existing EU financial services legislation. But, because of the complex nature of the specific items, the situation can be more complicated for hybrid tokens that incorporate more aspects of the archetypes (i.e. hybrid utility/investment tokens, hybrid currency/investment tokens, hybrid currency/investment/utility tokens)[25].

Having seen the two reasons behind the uncertainty of the EU regulation, even when a crypto-asset is qualified as a financial instrument there is a lack of clarity on how the existing regulatory framework will apply to such assets. Until now, the problem has always been the scoping of the regulatory framework, not the "performance". As the existing regulatory framework was not designed with crypto-assets as primary objective (crypto-assets were not a thing until much later), NCAs face these challenges in interpreting and applying the various requirements[26]. A practical example, NCAs are fighting a war without the latest technologies, and just like a ware, they are trying to cope with the situation at best they can. **The main problem is that the technology speed does not match the regulatory rhythm.**

5. Regulatory obstacles and gaps in the use of security tokens and DLT in the EU financial services legislation

As the existing regulatory framework was not designed with DLT in mind, there are some aspects in the existing legislation that may limit the usage of "security tokens" (for example, crypto-assets that can be addressed by the MiFID II, considering them as

[25] HACKER and THOMALE., (2017), *op. cit.*
[26] ESMA, (January 2019), *Advice on 'Initial Coin Offerings and Crypto-Assets*, ESMA (January 2019), *Advice on 'Initial Coin Offerings and Crypto-Assets*, electronically available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

financial instruments). If it's true that security token issuances have gained popularity and strength in numbers, there's still a lack of market infrastructures, platforms, practical usages, as well trading, clearing and settlement services for those security tokens.

The main problem and constrain to the expansion of the security token usage is in fact that without a secondary market able to provide liquidity, the primary market for security tokens will never expand in a sustainable way. In a recent survey, carried out by jointly by several organizations and companies (such as FD2A, AMAFI, AFG, ASPIM, Gide 255, Woorton, Consensys, PWC), 77% of the respondents answered that the possible implementation of a regulation can seriously jeopardize the development of security tokens in the EU[27]. The regulatory weaknesses, endangering the sustainable and responsible growth of crypto-assets in the financial services sector can be grouped into five categories.

The first issue, as already said, is represented by the impossibility to apply some specific EU rules to DLT (and to security tokens as well) as they were initially designed for traditional financial instruments. One example is the MiFID II reporting requirements.

The second issue is represented by the lack of legislation of some specific key areas of crypto-asset. These regulatory gaps exist because of the legal, technological and operational characteristics of the crypto-assets: they are surely heterogeneous, but surely they are very different from all the existing assets too[28]. **The fact that crypto-assets are so different by all the existing instruments/assets, currently there are no formal, reliable and, most importantly, specific** requirements for protocols, algorithms, smart contracts underlying DLT. For example, imagine that the software on which a smart contract is based is defective, inaccurately reflecting the parameters of the existing contract. Such errors can be devasting, and not so easy and immediate to resolve: the operations via smart contracts in fact are recorded on the DLT and would not be possible to cancel the errors. Surely, adjusting measures can be done to resolve the issues

[27] FD2A, AMAFI, AFG and ASPIM, (2019), *The FD2A, AMAFI, AFG and ASPIM measure the interest of actors for "security tokens". Questionnaire on security tokens – summary of results*, electronically available at: http://www.amafi.fr/download/pages/2qnY1c7mzJspXmuzqEZWD6blcihezxug2Vgpt32a.pdf.
[28] ESMA, (2019), *op. ult. cit.*

and consequences, but only after the phenomenon occurred, as it cannot have been prevented.

The underlying technology/algorithms/protocols surely is generating some new forms of cyber risks, which are totally unaddressed by the existing rules: as already mentioned, while having a copy of the same data on all the nodes in the network eliminates the risk of a central failure and/or a direct attack, it is indeed true that the security of the entire network remains dependent on its links. A potential attacker could exploit the weakest connects to infiltrate into the network.

As already said, the data could be safe from fraudulent manipulation, but normal users are not protected by potential fraudulent attacks (as scams). If the network is not composed by a lot of nodes/users, or if the attack is massive, the catastrophic effect is the possibility that all the DLT participants are corrupted at the same time. This phenomenon could destroy entire DLT networks, as there would be no countermeasures. Lastly regarding this specific point, as it may be true that the custody of private keys for accessing the usage of crypto-assets could be the equivalent of the 'safekeeping and administration of financial instruments for the account of clients' service under MiFID II, this activity is not currently regulated at any EU level.

Another huge issue interfering in the crypto-assets spreading is the impossibility to develop the necessary infrastructure for security token, because of the current EU rules preventing the development of financial market infrastructures (such as trading venues, central clearing counterparties (CCPs) and central securities depositaries (CSDs)) based on decentralized exchanges and permissionless DLT networks where activities are not entrusted to a central body.
This specific case is really a problem, as it is not possible even to apply MiFID II or SFD/CSDR rules to them as these rules require the existence of a trading venue operator or a CSD to safely operate the securities settlement system (and intermediaries, such as brokers/market members and CSD participants/custodians).

Regarding centralized/permission-based DLT network, some regulatory uncertainties and obstacles remain for market infrastructures that rely on them. Even when a central entity is clearly identifiable, the existing legislation does not fit well.

Such legal uncertainties are a concern not only for potential new entries, but also for existing authorized market players. In addition, the current regulation also prevents the extensive testing of DLT, in order to determine to what extent, the DLT technology is mature enough to replace or complete existing market infrastructures[29].

Existing rules jeopardize the development of financial market infrastructures which could potentially merge certain activities (trading, clearing, settlement and custody) The existing EU financial services legislation follows the lifecycle of a transaction (trading, clearing and settlement): it is required in fact the presence of authorized market intermediaries (such as broker, clearing members, custodians) and the related market infrastructures (a trading venue, CCP, CSD), consequently setting specific safety requirements on such entities. It is easy to notice that the usage of DLT, with all transactions recorded in a decentralized ledger, can de-bureaucratize and condense the normal steps (trading, clearing and settlement) to fast, real-time activities[30]: if a security is issued on a DLT, the DLT also recordkeeps the data, making CSDs superfluous. For CCPs, they would be superfluous too, as the majority of their functions would be performed by smart contracts.

This simplification of the multi-step trading process would improve efficiency, by reducing the entities intermediating, but also would reduce potential risks, such as errors risk and counterparty risk (by reducing the time periods).
By contrast, the usage of DLT and security tokens to operate the trade and post-trade processes at the same time would raise potential new risks, such as new forms of cyber risks, that are not currently mitigated by the existing EU rules.

6. Consumer and investor protection risks and risks of fraud (for unregulated crypto-assets)

At the current legislative state, for all the crypto-assets not qualified as MiFID II financial instruments or as electronic money under EMD2, the users purchasing and

[29] ESMA, (2019), *Report on Licensing of FinTech Business models*, cit.
[30] OECD, (2020), *The Tokenisation of Assets and Potential Implications for Financial Markets*, electronically available https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm.

utilizing them would not benefit and be protected by the EU legislation, exposing the customers to a range of relevant risks, as highly announced by the main NCAs and EBA since 2013[31] . In relation to potential and inherent customer risks, in 2017 many NCAs and ESMA published a warning study about initial coin offerings (ICOs) and crypto-assets[32]. The ICOs are an innovative way of raising money from the public: a business or individual issues a crypto-asset (often a cryptocurrency) and puts them for sale in exchange of traditional currencies, such as Euros or Dollars, but also for more stable virtual currencies as well, like Bitcoin.

The mechanism is exactly the same of IPOs for stocks: a new item is released to the public, the issuer gains an enormous amount of funds to further develop the item, and the public gets the opportunity to buy an asset with relevant growth potential. The particularity of ICOs, also in comparison to the IPOs, is the nature of the asset offered to the public. Some tokens in fact serve only to access or purchase a service/product that the issuer develops using the funds of the ICO (e.g. utility tokens), others.

The IPOs most similar case, provide voting rights or a share in the future revenues of the issuing venture (e.g. investment tokens), and some other have not a tangible value, but the value is the technology itself (e.g. some payment tokens). It is worth noting that when an offer concerns tokens qualifying as MiFID II financial instruments, the term "security tokens offerings" is often used: the term ICO in fact is used by the industry for marketing purposes to resemble IPO (initial public offering), as the general mechanism is the same, but the term 'token sale' would reflect better the substance of the phenomenon.

Three main risks can be clustered in relation to ICOs and more in general to crypto-assets acquisition by the general public.

1. **Consumers can purchase unsuitable products without having access to adequate information.** Crypto-asset issuances in fact are sometimes formalized in related "white papers", documents describing the crypto-assets and the ecosystem around it, just like the mandatory issue documents for IPOs on

[31] ESMA, SECURITIES AND MARKETS STAKEHOLDER GROUP, (2018), *Own initiative Report on initial coin offerings and crypto-assets*, electronically available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf.
[32] ESMA (January 2019), *Advice on 'Initial Coin Offerings and Crypto-Assets*, cit.

regulated stock exchanges. However, the ICOs white papers are not mandatory, and therefore not standardized (as opposed to similar documents in IPOs). The result is that the quality, transparency and disclosure of risks may vary greatly[33]: a huge number of "white papers" often feature exaggerated or misleading information, with the objective of attracting unaware investors and customers, who may not understand the rights but more importantly the risks associated with such crypto-assets. Such "white papers" have sometimes a much more "advertising" focus rather than an informative purpose, not mentioning volatility risks and the possible total loss of the amount invested. Currently this is allowed because of the lack of regulation on such documents.[34]

The result is consumers buying crypto-assets not suitable for their risk profiles and needs, often in searching for quickly high profits. The clear and ultimate example regarding this consumers' attitude would be the leverage trading of crypto-assets (usually cryptocurrency) on trading platforms. Leveraging is a form of margin trading in which the consumer borrows an amount of funds from the platform to buy a quantity of crypto-assets that is larger than he would be able to purchase without the "platform loan". If the price goes up, the profits are way higher than what they would be without the leverage, but the same goes for the losses, as the general functioning remembers the call-put stock options. The usage of such phenomenon is controversial: given the high fluctuations of crypto-assets prices in fact, most trading platforms nowadays are reluctant to offer such services, even if they are highly used be the final end users. In order to give an idea of the numbers involved, in accordance with a 2018 study performed by the University of Cambridge, some platforms offer leveraging from x2 to x100 with a median of x3.3[35].

---

[33] *Ibid*.

[34] HM TREASURY CRYPTOASSETS TASKFORCE, (October 2018), *Financial Conduct authority and Bank of England*: *final report*, electronically available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.

[35] RAUCHS, BLANDIN, KLEIN, PIETERS, RECANATINI and ZHANG, (December 2018), *2nd Global crypto-asset benchmarking study*, Cambridge Centre for Alternative Finance, electronically available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf.

2. **Consumers are also at risk of losses resulting from fraudulent activities.** As the issuance and offering of services related to crypto- assets are almost totally unregulated, this makes the market vulnerable to illicit usages of the technology, in particular exploiting the high-yield returns aura which the crypto-assets market today has, making it easy for fraudsters to attract customers and potential victims. While it is indeed true that fraudulent activity is homogeneously widespread across the vast range of crypto-assets, it is also different depending each category of the aforementioned. For instance, the higher risk of fraud is ICOs, due to the lack of regulation on such delicate events. The mechanism is really simple: ICOs are non-other than a release of a crypto-asset to the general public, but not on a regulated exchange. The result is that fraud estimates range from 5% to 25% of all ICO offerings[36], and in certain cases and categories up to 81%[37]. In some cases, the most famous ones, the developers/issuers disappear just after getting the funds through the ICO, as the crypto-assets do not exist at all or the current development phase is far from the status advertised before the ICO (in order to attract investors), lacking of an appropriate plan or capability to deliver the product or service[38]. In conclusion, the users' lack of understanding of the technical mechanism underlying the asset ends up boosting the risk of fraud.

3. **Consumers may also be at risk due to the immaturity or failings of service providers.** Even if the two risk layers activities described above are successfully completed, even if the crypto-asset release has been made, the final customers are subject to the everyday usage risk: as currently there are no legal minimum standards on operational risks (including products capability, but also cyber risks), the service providers are nor encouraged or obliged to put in place appropriate systems and controls, preventing customers by being subject to losses arising from hackers' attacks, software errors or data loss. The so-called **operative risks** can be clustered into two different categories:

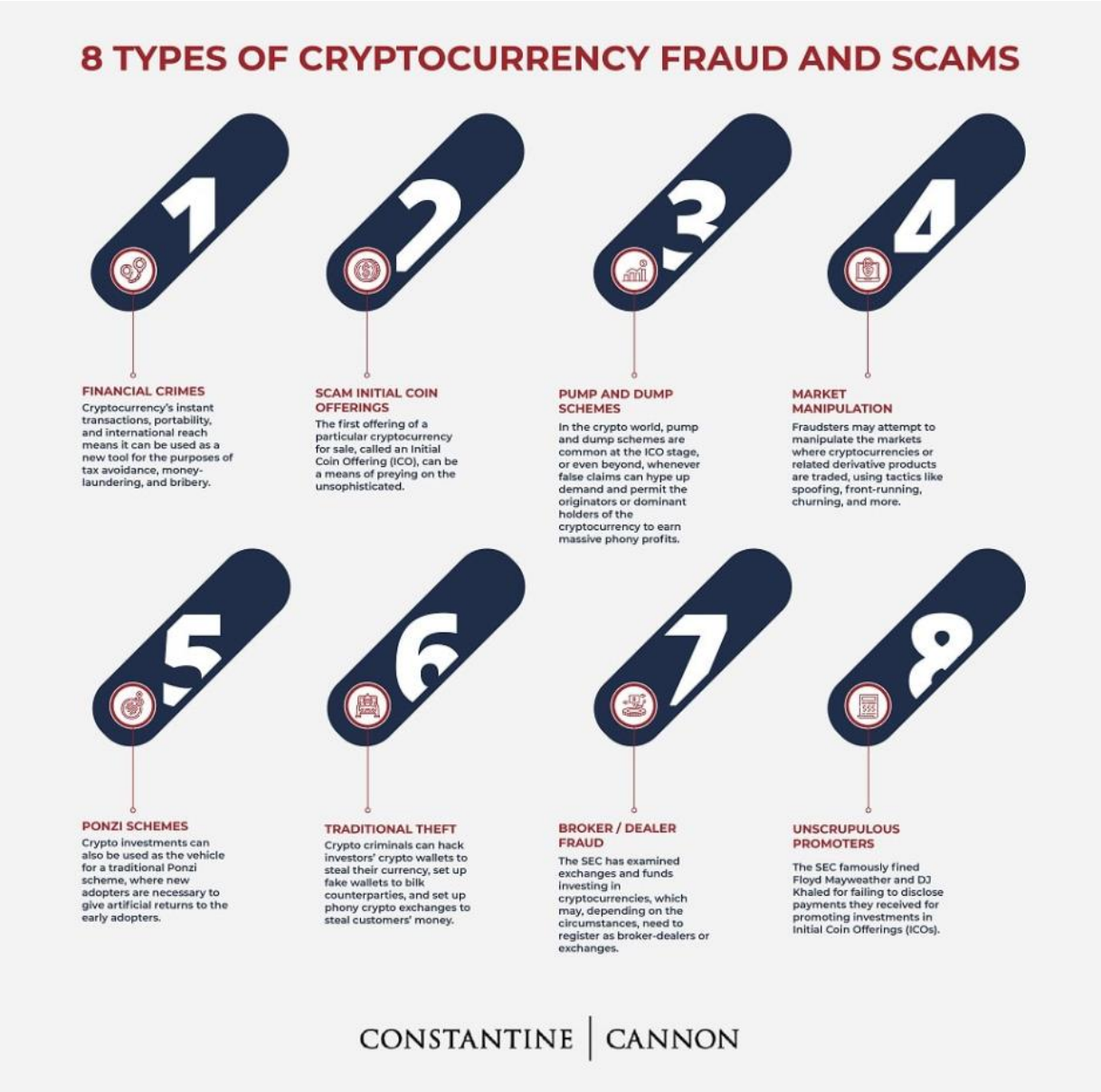
[36] CATALINI and GANS, (2018), *Initial Coin Offerings and the Value of Crypto Tokens*, electronically available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137213.
[37] DOWLAT and HODAPP, (2018), *ICO Quality: Development & Trading;* RAO and VATRAPU, (2021), *Distributed ledger technologies and blockchain for FinTech: Principles and applications*, *The Routledge Handbook of FinTech*, Routledge, p. 79 ff.
[38] ESMA, (2019), *Advice on 'Initial Coin Offerings and Crypto-Assets*, cit.

a. **Cyber hacks**: (e.g. to obtain users' private keys) as already said in the previous paragraphs can put consumers at risk of large losses, as crypto-assets are viewed as high-value targets for theft. The most recent and largest cyber-thefts performed to be remembered include Coincheck ($540 million stolen in January 2018), Mt Gox (nearly $500 million stolen in February 2014) and Bithumb ($32 million stolen in South Korea). These indeed are single, high-return thefts, but cannot be forgotten all the single scams and thefts to "normal" users performed every day.

b. **Operational issues**: consisting in temporary disruptions of systems (often due to activity peaks, and the ratio between servers' power and users not balanced), which can delay or deny consumers' access to their funds. During such conditions, holders of crypto-assets are not able to carry out transactions when they like and, in a market where the time is one of the most important things, more than in the stock market due to the really high volatility, may therefore suffer losses due to fluctuations during that period. It happened that some trading platforms or exchanges have stopped trading and users have lost their entire holdings, in case of extreme fluctuations (ShibaInu coin rally, for example)[39]. In addition, due to the operational platform delay it could occur in high peak usage periods, and being the fees often calculated on the spread between the buying and selling prices, some service providers can charge higher and variable fees that are not properly disclosed to consumers, as the transactions are delayed by few moments, resulting in less convenient purchasing or selling price. Solving these kind of consumer conflicts can be difficult, especially for platform using an external customer care support, often offering just one or two languages, and offering no internal standard procedures for handling complaints[40].

[39] FMA, (2018), *Bitcoin & Co*, electronically available at: https://www.fma.gv.at/en/fintech-point-of-contact-sandbox/fintech-navigator/bitcoin-co/.

[40] CNMV and BANCO DE ESPAÑA, (2018), *Joint press statement on 'cryptocurrencies' and initial coin offerings*, electronically available at: https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/presbe2018_07en.pdf.



Costantine Cannon, Cryptocurrency Fraud, electronically available at: https://constantinecannon.com/practice/whistleblower/whistleblower-types/financial-investment-fraud/cryptocurrency-fraud/

CHAPTER II

ENTITIES UNDER THE SCOPE OF MiCAr

1. What could change in practice for the Service Providers

1.1. CASP introduction

According to the to the text proposed by the Commission, service providers (referred also as CASP, *Crypto-Asset Service Providers*) are considered «any person whose occupation or business is in the provision of one or more crypto-asset services to third parties on a professional basis»[41], resulting in the fact that «Crypto-asset services shall only be provided by legal persons that have a registered office in a Member State of the Union and that have been authorized as crypto-asset service providers in accordance with Article 55»[42]. The comparison of such definitions used by the Commission and the one reported in the Article 4 of MIFID II, regarding the *Investment Firm*[43], is quite straightforward: the only difference is given by the fact that, unlike MIFID II, MiCAr does not allow Member States to comprehend non-legal persons in the crypto-assets service providers group.

The first decision made by the Commission in formalizing the MiCAr approach to CASP is the division of such category into two groups:

A. **Trading platforms providers**

A.1. Service providers responsible for the management of the platform used to store the crypto-assets (the so-called "wallets"), and the property of the cryptographic keys used to assure the safety of the funds stored. Simplifying, their services can be summarized as «custodians of the wallets, in which the funds are stored»[44].

[41] Art 3 (8), MiCAr.
[42] Art 53 (1), MiCAr.
[43] Art 4, MIFID II.
[44] Art 3 (9) (10), MiCAr.

A.2. Service providers responsible for the property, management and administration of the trading platforms (the so-called "*crypto exchanges*"), allowing crypto-crypto and crypto-fiat exchanges. They are responsible for the process of funds exchange between the accounts rather than the safe custody of the funds[45]. However, it is worth noting that currently most of the crypto exchanges also offer crypto-assets funds custody services, with their own, integrated, wallets.

B. Crypto-assets usage intermediaries:

B.1. Service providers responsible of placing and execution of orders (buy or sell). They can be considered as crypto-assets brokers, managing third-party crypto-funds[46].

B.2. Service providers responsible for advising services, regarding operations such as acquisitions, sales or usages of the crypto-assets funds[47].

While it is true that this classification is formalized, it is also clear that no distinction in the articles is made regarding the group 1 or group 2: currently, all the articles regulating the CASP are affecting the whole category, but due to the continuous changing nature of the topic treated, it is not clear if such differentiation will make a difference in the Member States application of the MiCA regulation.

Continuing the comparison between the MiCAr and MIFID II approaches in defining the CASP and the services provides, the differences between them are very few, as it is noticeable that the services (based on the distinction of CASP subgroups) are closely related to the services defined in the Annex I Section A of the MIFID II, with the sole, obvious (because of their technology-specific nature), exception of the "*wallet providers*". Moreover, even for "*wallet providers*", the Commission used the «*safekeeping and administration of financial instruments for the account of clients, including custodianship and related services*» reported in the MIFID II as a clear example in defining guidelines for the regulation of entities providing «funds (whether electronic, crypto or fiat) safekeeping, custody and administration» as a service. Generally speaking,

[45] Art 3 (11), MiCAr.
[46] Art 3 (14) (15) (16), MiCAr.
[47] Art 3 (17), MiCAr.

the services listed by the Commission are the same services illustrated by the Financial Action Task Force (FATF, an independent inter-governmental body that develops and promotes policies to protect the global financial system) in their *Virtual Assets and Virtual Asset Service Providers* risk-based guide of the 2019[48].

Concluding the introduction to CASP, it is worth noting and remembering that the Commission proposal defines the guidelines and general rules to be followed by the CASP, adopting a model *service oriented* and not *asset specific*. The Commission, in fact, is regulating the CASP services provided by the customers, apparently disregarding the different nature of the crypto-assets subject to the specific services. In order to mitigate the drawback of such regulating model, the Commission specified that further requirements could be added for particular types of crypto-assets, in particular stating that «depending on the services they provide and due to the specific risks raised by each type of services, crypto-asset service providers should be subject to requirements specific to those services. Crypto-asset service providers providing the service of custody and administration of crypto-assets on behalf of third parties should have a contractual relation with their clients with mandatory contractual provisions and should establish and implement a custody policy. Those crypto-asset service providers should also be held liable for any damages resulting from an ICT-related incident, including an incident resulting from a cyber-attack, theft or any malfunctions»[49].

The specific articles, as said divided by service-type, will be subject of an in-depth analysis in the next paragraphs.

1.2. CASP authorization

Before going into details of the specific regulations for the different service categories, it must be defined the Commission's approach in determining the requirements for CASP authorization process. In fact, as previously said, the Commission adopted the same principals used in MIFID II for investment firms, defining an

[48] FATF (2019), *Guidance for a risk-based approach: virtual assets and virtual asset service providers*, electronically available at: "https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.
[49] Recital 59, pag. 27, MiCAr.

authorization scheme for CASP in order for them to be able to operate in the crypto-market.

More specifically, and as already seen in the CASP definition, the crypto-asset services should only be provided by legal persons, but this is not the only limitation, as two further requirements are set for CASP eligibility.

The first requirement is that such legal person must possess a registered office in one of the EU's Member State[50].

The second, and stricter, requirement set in MiCAr's Article 53 (first point) is that such legal person, in order to be considered a CASP (being able to provide crypto-assets services), must be authorized by the NCA (national competent authority) of the EU's Member State where the office is registered, in accordance to requirements illustrated in the Article 55[51]. Once authorized, in addition, the CASP must at all times meet the conditions for being a CASP. The same Article also specifies that «no person who is not a crypto-asset service provider shall use a name, or a corporate name, or issue marketing communications or use any other process suggesting that he or she is authorised as a crypto-asset service provider or that is likely to create confusion in that respect», a very important prohibition which gives the idea of how much the MiCA regulation proposal is customer-protection oriented.

The Commission also sets parameters and requirements for guiding the aspiring CASP applications, always following the general "high disclosure" principle, in order to detect suspicious/dubious applications made by inadequate legal persons, preventing their entrance into the crypto-market and maintaining the crypto-market integrity.
Such application parameters and requirements are extensively illustrated in the articles 54 and 55:

- The application must contain **general personal information** on the legal person, in particular its name, office legal address, website, legal status and its articles of association[52];

[50] Recital 50, pag. 25, MiCAr.
[51] Art 53 (1), MiCAr.
[52] Art 54 (2a, 2b, 2c), MiCAr.

- The application must contain **information on the services** planned to be provided to the market, as well as a **formal business plan**[53];

- The application must contain information and proofs about the **absence of any criminal records** (in particular: commercial, insolvency, financial, money-laundering and terrorism related laws) for any physical person in the aspiring CASP management or above the 20% (directly or indirectly) property threshold[54];

- The application must contain **information certifying that the management possess the adequate knowledge, skills and experience** to correctly manage the company's services[55]. This is a clear example of the customer-protection orientation of the MiCA regulation;

- The application must contain adequate information about policies and procedures in relation to the **internal control system of the applicant**, as well as **documents regarding risk assessments**, **business continuity plans**[56] and **complaints from clients**. This kind of information has to secured by a specific system in order to ensure its integrity and confidentiality[57];

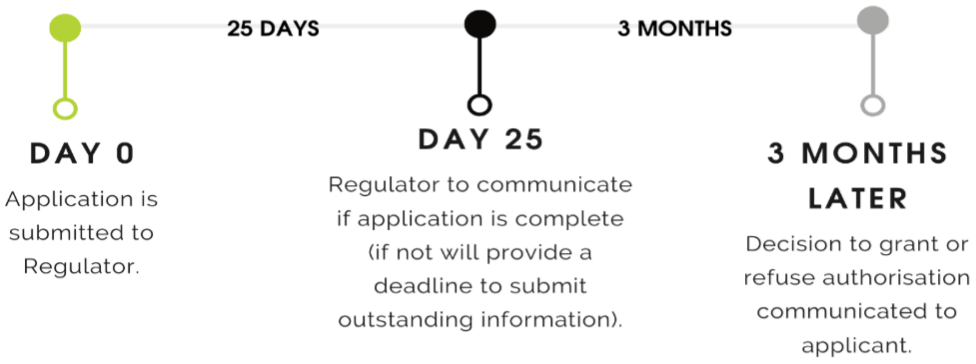
- The application must contain evidence of the **prudential safeguards** that CASP is subject to in order to prove them to the NCA[58];

- The application must contain information regarding **procedures and system to uncover clients' market abuse** and **procedure for the segregation of funds and crypto-assets of the clients**;

[53] Art 54 (2d, 2e), MiCAr.
[54] Art 54 (2f), MiCAr.
[55] Art 54 (2g), MiCAr.
[56] Art 54 (2h), MiCAr.
[57] Art 54 (2k), (2i), MiCAr.
[58] On this matter, see Section 5.3.3. of MiCAr.

- The application has to contain **information pursuant to the MiFID II, EMD2, PSD2 or the nation law appropriate to crypto-asset services** before the entry into effect of the MiCA regulation. The applicant doesn't have to resubmit this kind of information in case the NCA already has it accessible and up-to-date[59].

If the application results as "complete" to NCA, within 25 working days communication must be establishes with the applicant. Otherwise, if the application is found to be "incomplete", the NCA shall set a deadline in order to submit the outstanding information. If the application remains incomplete after this deadline, the NCA shall refuse the authorization[60].



MiCA explained: the EU crypto-asset law. The proposed Markets in Crypto-asset Regulation - XReg Consulting LTD

Furthermore, under any circumstances, if the application is "complete" the NCA has to immediately let the applicant know[61]. In fact, the art. 55 of MiCAr states that the NCA, in any case, within 3 months of receipt of the complete application must strive, taking into account the complexity and the nature of the services the applicant plans to provide – in order to adopt a well-thought-out decision whether to grant or refuse the authorization[62]. When the decision is made, the NCA has to inform the applicant within 3 working days[63]. If the decision is favorable, the authorization must contain the specific services the CASP is authorized to provide[64].

[59] Art 54 (3), MiCAr.
[60] Art 55 (1) and (2), MiCAr.
[61] Art 55 (3), MiCAr.
[62] Art 55 (5), MiCAr.
[63] Art 55 (7), MiCAr.
[64] Art 53 (2), MiCAr.

Even though the MiCA regulation states that CASP's authorization must be considered as "valid" for the entire European Union (through which a CASP provides its services without the necessity of having a physical presence in the territory of a host Member State[65]), MiCAr also introduces a *passporting-regime* that has a notification requirement very similar to the one provided in the MiFID II for investment firms[66].

In fact, following this kind of regime, CASP is obliged to draw up a list containing:

- The EU States in which it is planned to provide its services;
- The starting date of the intended provision;
- The activities CASP provides but that are not covered by MiCA regulation[67].

After CASP submits this list, the NCA has to communicate – within 10 working days – the information listed to the host EU member States, to ESMA and to EBA. Of this communication the NCA must immediately, without any delay, advise the notifying CASP. This advice – that has to be received at the latest 15 days after having submitted the notification to the NCA – is essential to CASP because only after receiving this information from the NCA, it is allowed to provide its services[68].

That is the reason why if CASPs intend to provide their services cross-border and this is not being notified to their home NCA of this intention, CASPs are obliged to inform NCA and wait for its communication (or the latest 15 days after the submission of the advice) before being allowed to provide services in other Member States.

This NCA's authorization to be a CASP for any crypto-asset services, however, doesn't allow the provision of payment services related to those services because, in order to provide even this payment service, the PSD2 states that an additional authorization is needed. In fact, to be a payment institution, the CASP needs to be authorized to be legally able to provide this kind of service[69]. That is why all CASPs authorized in the EU must be inscribed by ESMA (which is informed by the NCA of all authorizations granted to the CASP[70]) in a public register with the following information about the CASP:

- Its name;
- Its legal status;

[65] Art 53 (3), MiCAr.
[66] On this particular matter, see Art 34 MiFID II.
[67] Art 58 (1), MiCAr.
[68] Art 58 (4), MiCAr.
[69] Recital 58 of Art 63 (4), MiCAr.
[70] Art 55 (6), MiCAr.

- Its physical address;
- All crypto-asset services it is authorized to provide;
- The EU States in which the CASP aims to provide the services.

Because every authorized CASP is listed in this public register, every person who is not authorized as a CASP must refrain from using any name, strategy or process that could mislead the public suggesting being authorized as such[71]. Nonetheless, leaving aside the matter of unauthorized people to be a CASP, authorization requirements of the MiCAr work partially different for credit institution and investment firms.

As a matter of fact, the latter are partly exempted from MiCAr's scope itself. In fact, credit institution already authorized under the CRD-IV to provide crypto-asset services and investment firms authorized under the MiFID II, are not subject to further authorization requirements under the MiCAr in order to provide crypto-asset services[72]. They still need to be included in the European *passporting regime* and the previously mentioned ESMA's public register of CASPs[73].

1.3. CASPs' general obligations

CASPs must assure financial stability, market integrity and consumer protection[74].

On one hand, in order to ensure the latter, all CASPs shall follow some general **rules of conduct**, such as the obligation to act fairly, honestly and professionally in the best interest of the clients. To achieve this aim, all CASPs must inform clients in a non-misleading way by:

- making clear their pricing policies (they should be put on a prominent place on the website);
- informing them of every risk associated with the purchase of crypto-assets[75];
- establishing a complaint handling procedure[76];

[71] Art 53 (1), subpara 3, MiCAr.
[72] Recital 54, MiCAr.
[73] On this particular matter, see Art 2 (5), Recital 54 and (6), MiCAr.
[74] Recital 55, MiCAr.
[75] Art 59, MiCAr.
[76] Art 64, MiCAr.

- having a strong and efficient policy that aims to identify, manage and disclose any possible conflict of interest[77].

On the other hand, in order to ensure financial stability and market integrity, CASPs shall also respect **prudential requirements** such as maintain sufficient capital in one of these 2 forms[78]:

1. Own funds «consisting of Common Equity Tier 1 items referred to in Articles 26 to 30 of Regulation (EU) No 575/2013»[79];
2. Adequate «insurance policy covering the territories of the Union where crypto-asset services are actively provided or a comparable guarantee»[80].

In fact, CASPs must have – always, at all times – funds equal to, or higher than[81], either of the following:

A. The minimum capital requirements established by MiCAr's Annex IV that identifies 3 classes of services based on the nature of the specific crypto-asset services provided:

- Class 1: a minimum of €50.000,00 for CASPs authorized for the transmission and reception of orders on behalf of third parties and/or providing advice on crypto-assets and/or execution of orders on behalf of third parties and/or placing of crypto-assets;
- Class 2: a minimum of €125.000,00 for CASPs authorized for any class 1 crypto-asset services and custody and administration of crypto- assets on behalf of third parties;
- Class 3: a minimum of €150.000,00 for CASPs authorized for any class 2 crypto-asset services and the exchange of crypto-assets for official currency or other crypto-assets and/or the operation of a trading platform for crypto-assets.

B. ¼ of the fixed overheads of the previous year (which has to be annually reviewed). «Crypto-asset service providers that have not been in business for one year from the date on which they started providing services shall use, for calculation the

[77] Art 65, MiCAr.
[78] Art 60 (2), (4) and (5), MiCAr.
[79] Art 60 (2), MiCAr.
[80] *Ibid.*
[81] Art 60 (1), MiCAr.

projected fixed overheads included in their projections for the first 12 months' of service provision»[82], as submitted with the application for the authorization.

After having established those prudential requirements at Art. 60, in the following Article MiCAr defines thorough **organizational requirements** for all CASPs. The Article states that «members of the management body of crypto-asset service providers shall have the necessary good repute and competence, in terms of qualifications, experience and skills to perform their duties»[83]. The following Article establishes that the NCA has to be notified if anything changes in the management body[84]. Another requirement for CASPs regards the fact that employees «shall demonstrate that they are capable of committing sufficient time to effectively carry out their functions»[85] and that they are free of convictions of offences relating to money laundering or terrorist financing or other financial crimes[86].

This is a necessary requirement because MiCA regulation also establishes that CASPs must «employ personnel with the skills, knowledge and expertise necessary»[87] to discharge the responsibilities allocated to them. In fact, «the management body» is in charge of assessing and periodically reviewing «the effectiveness of the policies arrangements and procedures put in place to comply with its obligations»[88] and of taking «appropriate measures to address any deficiencies»[89]. Moreover, CASPs personnel has to ensure continuity and regularity in the performance and the delivery of their crypto-asset services to clients along with the establishment of an effective business continuity policy and disaster recovery plans, primarily with the employment of «resilient and secure ICT

[82] Art 60 (3), MiCAr.
[83] Art 61 (1), MiCAr.
[84] Art 62, MiCAr.
[85] Art 61 (1), MiCAr.
[86] Art 61 (3), MiCAr.
[87] Art 61 (4), MiCAr.
[88] Art 61 (5), MiCAr.
[89] *Ibid*; Art 61 (7) of MiCAr also establishes that those control mechanisms and effective procedures for risk assessment and for the safeguard of security, integrity and confidentiality of information must be constantly implemented.

systems in accordance with Regulation (EU) 2021/xx[90] of the European Parliament and of the Council»[91].

CASPs also must have «systems and procedures to safeguard the security, integrity and confidentiality of information»[92] that must be supervised by NCAs through the analysis of the records that CASPs must keep of «all crypto-asset services, orders and transactions undertaken by them»[93]. These records «shall be sufficient to enable competent authorities to fulfil their supervisory tasks and to perform the enforcement actions, and in particular to ascertain whether the crypto-asset service provider has complied with all obligations including those with respect to clients or potential clients and to the integrity of the market»[94]. Therefore, CASPs have to implement also «systems, procedures and arrangement to monitor and detect market abuse» committed by clients in order to be able to «immediately report to their competent authority any suspicion that there may exist circumstances that indicate that any market abuse has been committed or is likely to be committed»[95].

Moreover, Article 63 of MiCA regulation – regarding the safekeeping of clients' crypto-assets and funds – states that CASPs «that hold crypto-assets belonging to clients or the means of access to such crypto-assets» are obliged to make «adequate arrangements» in order to «safeguard the ownership rights of clients, especially in the event of the crypto-asset service provider's insolvency, and to prevent the use of a client's crypto-assets on own account except with the client's express consent». CASPs also have to «safeguard the rights of clients and prevent the use of clients' funds, as defined under Article 4 (25) of Directive (EU) 2015/2366[96], for their own account»[97], if their business

[90] In MiCAr's note n. 63 it is stated that it regards the «Proposal for a Regulation of the European Parliament and the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 – COM (2020)595».
[91] Art 61 (6), MiCAr.
[92] Art 61 (7), MiCAr.
[93] Art 61 (8), MiCAr.
[94] *Ibid.*
[95] Art 61 (9), MiCAr.
[96] MiCAr's note n. 67 explains that this is «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 (OJL 33, 23.12.2015, p.35) ».
Article 4 (25) states that «'funds' means banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC».
[97] Art 63 (1) and (2), MiCAr.

models or the crypto-assets services require holding clients' funds. In other words, if the business model requires the CASP to hold clients' funds as defined in the PSD2[98], these funds must be arranged with a credit institution or a central bank segregated from the CASP's own funds[99], unless the CASP has been authorized as a payment institution under the PSD2 or as an electronic money institution under the EMD2[100].

Needlessly to say, it should be allowed to CASPs to outsource the performance of operational functions to third parties. However, Article 66 of MiCA regulation states that if they do so, they must «take all reasonable steps to avoid additional operational risk» and «shall remain fully responsible for discharging all of their obligations»[101] to third parties. For these reasons, the CASP's agreement with the third party involved in the outsourcing[102] shall ensure at all times that all the following conditions are complied with:

- Outsourcing cannot result in the delegation of the responsibility of the CASP nor the alteration of the relationship between the CASP and its clients nor the conditions for the authorization[103];

- CASP must guarantee that third parties involved in the outsourcing cooperate with the «competent authority of the crypto-asset service providers' home Member State» (i.e., the NCA). The outsourcing cannot «prevent the exercise of supervisory functions by those competent authorities, including on-site access to acquire any relevant information needed to fulfil those functions»[104];

- CASP shall «retain the expertise and resources necessary for evaluating the quality of the services provided, for supervising the outsourced services effectively and for managing the risk associated with the outsourcing on an ongoing basis»[105];

[98] On this matter, see Art 45 (25), PSD2.
[99] Art 63 (2) and (3); Recital 58, MiCAr.
[100] Art 63 (5), MiCAr.
[101] Art 66 (1), MiCAr.
[102] Art 66 (3), MiCAr.
[103] Art 66 (1 a), (1 b) and (1 c), MiCAr.
[104] Art 66 (1 d), MiCAr.
[105] Art 66 (1 e), MiCAr.

- CASP must have «direct access to the relevant information of the outsourced services»[106] and «ensure that third parties involved in the outsourcing meet the standards laid down in the relevant data protection law» (i.e., most importantly provided by the General Data Protection Regulation or GDPR[107]) «which would apply if the third parties were established in the Union»[108].

1.4. CASP's obligations for the provision of specific crypto-asset services

The third Chapter of the Title V of MiCA regulation regards the "*Obligations for the provision of specific crypto-asset services*" by such meaning:

- Custody and administration of crypto-assets on behalf of third parties (Article 67, MiCAr);
- Operation of a trading platform for crypto-assets (Article 68, MiCAr);
- Exchange of crypto-assets against official currency or against other crypto-assets (Article 69, MiCAr);
- Execution of orders for crypto-assets on behalf of third parties (Article 70, MiCAr);
- Placing of crypto-assets (Article 71, MiCAr);
- Reception and transmission of orders on behalf of third parties (Article 72 MiCAr);
- Advice on crypto-assets (Article 73, MiCAr).

The primary aim of the above-mentioned obligations is to reduce the typical risk posed by the provided service.

In particular, the first obligation for the provision of specific crypto-asset services, which is the **custody and administration of crypto-assets on behalf of third parties** aim is to minimize the risk of loss of the crypto-assets that are administered and held for the CASPs clients[109]. In fact, above all, MiCA regulation states that the CASP must enter

[106] Art 66 (1 f), MiCAr.
[107] That is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[108] Art 66 (1 g), MiCAr.
[109] On this particular matter, see XREG CONSULTING LTD, (2020), *MiCA explained: the EU crypto-asset law. The proposed Markets in Crypto-asset Regulation*, p. 25 , electronically

into a contractual relation with their clients and provides mandatory provisions specifying the duties and responsibilities of the CASP[110], such as the nature and the description of the service provided, the identity of the parties, the description of the security system and the fees that CASP applies. Furthermore, Article 67 of MiCA regulation implies that «Crypto-asset service providers that are authorised for the custody and administration of crypto-asset on behalf of third parties shall segregate holdings on behalf of their clients from their own holdings. They shall ensure that, on the DLT, their clients' crypto-asset are held on separate addresses from those on which their own crypto-assets are held»[111].

The CASP also has the duty to ensure that the crypto-assets are returned as soon as possible to its clients and to assure that, CASP must have a custody policy with internal rules and procedures in order to ensure the safekeeping and the control of the client's crypto-assets[112]. This custody policy must be demonstrated to the NCA in the application of the CASP[113]. In fact, MiCA regulation establishes the duty[114] for CASPs to ensure to clients that their crypto-assets – and the rights related to them due to cyber threats, negligence or frauds – will get lost. Article 67 states that, CASP «that are authorized for the custody and administration of crypto-assets on behalf of third parties» must indeed be liable – in the terms above mentioned – to their clients as a result from a «malfunction or hacks up to the market value of the crypto-assets lost»[115]. This liability rule holds CASPs liable even if the loss is the result of an external event beyond the CASPs' reasonable control.

In order to demonstrate their liability CASPs also must:

- keep a register to record movements, to register all clients' positions and to ensure that every movement is matched by a transaction[116];

available at https://uploads-ssl.webflow.com/5df7642ffbd9264804671001/5f7b3b3116ebd4add01abd32_XReg%20EU%20MiCA%20explained%20-issue%201-1.1a%20-FINAL.pdf.

[110] Art 67 (1); Recital 58, MiCAr.

[111] Art 67 (7), MiCAr.

[112] Art 67 (3), MiCAr.

[113] Art 54 (2 n), MiCAr.

[114] In fact, Art 67 (3 subpara 2), MiCAr states that CASPs «shall ensure that the crypto-asset service provider cannot lose clients' crypto-assets».

[115] Art 67 (8), MiCAr. This kind of liability is extremely strict and is in contrast to the liability rule for custodians safeguarding reserve assets of an issuer of ART, which will be subject of the next paragraphs.

[116] Art 67 (2), MiCAr.

- facilitate the clients' exercise of the rights attached to their crypto-asset (if certain rights are attached to it) and record any event which is likely to modify or create modifications in the clients' position register[117];
- inform their clients of their crypto-assets mentioning those concerned, their value, their balance and the transfers occurred during the period concerned at least once every three months and whenever the clients request to be informed as such[118].

The second category of obligations for the provision of specific crypto-asset services is regulated by Article 68 of MiCA regulation. The specific service in question is the **operation of a trading platform for crypto-assets**. Applicant CASPs that are willing to operate a trading platform for crypto-assets must describe – in their application – their operating rules in order to be given the authorization[119]. Besides this requirement, MiCAr includes further special obligations regarding transparency, systems, arrangements and procedures all designed to mitigate the specific risks that the operation of trading platform for crypto-assets could pose[120]. For this reason, CASPs must «lay down operating rules for the trading platform» that must «set the requirements, due diligence and approval processes that are applied before admitting crypto-assets to the trading platform»[121] and shall also «define exclusion categories, if any, which are the types of crypto-assets that will not be admitted to trading on the trading platform, if any»[122]. Furthermore, these operating rules must state that a crypto-asset should not be admitted to trading in case a white paper compliant with MiCA regulation has not been published, except the case in which the issuer is exempted from this obligation[123].

In order to mitigate financing of terrorism risk and money-laundering, these operating rules must also prevent the admission to trading of crypto-assets with an inbuilt anonymization function – the so-called *privacy coins* – «unless the holders of the crypto-assets and their transaction history can be identified by the crypto-asset service providers that are authorized for the operation of a trading platform for crypto-assets or by

[117] Art 67 (4), MiCAr.
[118] Art 67 (5), MiCAr.
[119] Art 54 (2 o), MiCAr.
[120] Recitals 59 and 60, MiCAr.
[121] Art 68 (1 a), MiCAr.
[122] *Ibid.* (1 b), MiCAr.
[123] On this particular matter, see Art 68 (1) subpara 2, MiCAr.

competent authorities»[124]. By doing so, MiCA regulation lays out a thorough pre-admission due diligence obligation for the CASPs that have to «ensure that the crypto-asset complies the operating rules of the trading platform and assess the quality of the crypto-asset concerned»[125], including those crypto-assets whose issuers is exempted to draw up and publish a white paper. When doing this quality-check to the crypto-assets, MiCAr states that the «trading platform shall take into account the experience, track record and reputation of the issuer and its development team»[126].

Regarding the time after the initial admission to trading on the trading platform, MiCAr establishes that CASPs have – in their operating rules – the obligation to «set conditions for crypto-asset to remain accessible for trading, including liquidity thresholds and periodic disclosure requirements»[127] to the issuers.

The already above-mentioned operating rules require also to «set out the policies, procedures and the level of fees, if any, for the admission of trading of crypto-assets to the trading platform»[128]; to «set conditions under which trading of crypto-assets can be suspended»[129] and to «set objective and proportionate criteria for participation in the trading activities, which promote fair and open access to the trading platform for clients willing to trade»[130]. Moreover, the operating rules shall «set requirements to ensure fair and orderly trading»[131] and «set procedures to ensure efficient settlement of both crypto-asset transactions and fiat currency transactions»[132].

Regarding transparency and information requirements, however, the CASPs are obliged to draft the above-mentioned operating rules «in one of the official languages of the home Member States or in another language that is customary in the sphere of finance»[133] and to make these rules public on their website.

MiCAr also establishes that «Crypto-asset service providers that are authorised for the operation of a trading platform for crypto-assets shall make public any bid and ask prices and the depth of trading interests at those prices which are advertised for crypto-assets through the systems of the trading platform for crypto-assets. The crypto-asset

[124] Art 68 (1) subpara 4, MiCAr.
[125] Art 68 (1) subpara 3, MiCAr.
[126] *Ibid.*
[127] Art 68 (1 f), MiCAr.
[128] Art 68 (1 c), MiCAr.
[129] Art 68 (1 g), MiCAr.
[130] Art 68 (1 d), MiCAr.
[131] Art 68 (1 e), MiCAr.
[132] Art 68 (1 h), MiCAr.
[133] Art 68 (2), MiCAr.

service providers concerns shall make that information available to the public during the trading hours on a continuous basis»[134]. CASPs also must make «public the price, volume and time of the transactions executed in respect of crypto-assets traded on their trading platforms. They shall make details of all such transactions public as close to real-time as is technically possible»[135]. In fact, MiCAr lays down the requirement for CASPs to make the information «available free of charge 15 minutes after publication in a machine readable format and remain published for at least 2 years»[136] and to «ensure that their fee structures are transparent, fair and non-discriminatory and that they do not create incentives to place, modify or cancel orders or to execute transactions in a way that contributes to disorderly trading conditions or market abuse»[137].

Moreover, with regards to the systems, procedures and arrangements, CASPs that are authorized to operate a trading platform for crypto-assets shall additionally ensure that their trading systems:

a) «are resilient;
b) have sufficient capacity to ensure orderly trading under conditions of severe market stress;
c) are able to reject orders that exceed pre-determined volume and price thresholds or are clearly erroneous;
d) are fully tested to ensure that conditions under points (a), (b) and (c) are met;
e) are subject to effective business continuity arrangements to ensure continuity of their services if there is any failure of the trading system»[138].

MiCA regulation further establishes that «Crypto-asset service providers that are authorised for the operation of a trading platform for crypto-assets shall not deal on own account on the trading platform for crypto-assets they operate, even when they are authorised for the exchange of crypto- assets for fiat currency or for the exchange of crypto-assets for other crypto-assets»[139] and that CASPs shall also «maintain resources

[134] Art 68 (5), MiCAr.
[135] Art 68 (6), MiCAr.
[136] Art 68 (7), MiCAr.
[137] Art 68 (9), MiCAr.
[138] Art 68 (4), MiCAr.
[139] Art 68 (3), MiCAr.

and have back-up facilities in place to be capable of reporting to their competent authority at all times»[140].

As a further operational obligation, the Commission's proposal also lays down that CASPs «shall complete the final settlement of a crypto-asset transaction on the DLT on the same date as the transactions has been executed on the trading platform»[141].

The third specific service that MiCAr regulates is the one regarding the **exchange of crypto-assets against official currency or against other crypto-assets**. In fact, MiCA regulation states that CASPs «that are authorized for exchanging crypto-assets against fiat currency or other crypto-assets shall establish a non-discriminatory commercial policy that indicates, in particular, the type of clients they accept to transact with and the conditions that shall be met by clients»[142]. This policy must be described already in the application for the authorization itself[143].

Pricing policy, however, are given by MiCAr that gives CASPs two options. The first one, is to publish a firm price of the crypto-assets and the second one is to establish a method for determining the price of the crypto-assets[144]. Regardless of CASPs decision, the transaction must be executed at the prices displayed at the time of the clients' orders' receipt[145]. Furthermore, CASPs «shall publish the details of the orders and the transactions concluded by them, including transaction volumes and prices»[146].

The fourth category of obligations is connected to the service of the **execution of orders for crypto-assets on behalf of third parties** can be found in Article 70 of MiCAr. This Article states that CASPs that execute orders for crypto-assets on behalf of third parties «shall take all necessary steps to obtain, when executing orders, the best possible result for their clients taking into account the best execution factors of price, costs, speed, likelihood of execution and settlement, size, nature or any other consideration relevant to

[140] Art 68 (3), MiCAr.
[141] Art 68 (8), MiCAr.
[142] Art 69 (1), MiCAr.
[143] Art 54 (2 p), MiCAr.
[144] Art 69 (2), MiCAr.
[145] Art 69 (3), MiCAr.
[146] Art 69 (4), MiCAr.

the execution of the order, unless the crypto-asset service provider concerned executed orders for crypto-assets following specific instructions given by its clients»[147].

To achieve this goal, CASPs must implement effective execution arrangements that provide fair, efficient and prompt execution and take every necessary steps to prevent possible misuse of their employees of any information regarding the clients' order[148]. Furthermore, CASPs «shall provide appropriate and clear information to their clients on their order execution policy and any significant change to it»[149].

The fifth category of obligations regulated by MiCAr relates to the **placing of crypto-assets**. This service can be provided only for two types of crypto-assets: crypto-assets that are already issued but that are not admitted to any trading platform and crypto-assets that are newly issued[150]. MiCA regulation gives CASPs providing the placing of crypto-assets some pre-contractual transparency obligations to be subject to. In fact, Article 71 states that before concluding the contract CASPs must communicate «to the issuer or any third party acting on their behalf»[151] the following information:

- «the type of placement considered, including whether a minimum amount of purchase is guaranteed or not»[152];
- «an indication of the amount of transaction fees associated with the service for the proposed operation»[153];
- «the considered timing, process and price for the proposed operation»[154];
- «information about the targeted purchasers»[155].

MiCA regulation also stats that CASPs providing this service «shall obtain the agreement of the issuers or any third party acting on their behalf »[156] regarding the type of placement, applicable guarantees by the CASP to a minimum purchase amount and if no guarantee is granted, an agreement to the that fact, as well as to the targeted

[147] Art 70 (1), MiCAr.
[148] Art 70 (2), MiCAr.
[149] Art 70 (3), MiCAr.
[150] On this particular matter see Art 3 (3), (15), MiCAr.
[151] Art 71 (1), MiCAr.
[152] Art 71 (1 a), MiCAr.
[153] Art 71 (1 b), MiCAr.
[154] Art 71 (1 c), MiCAr.
[155] Art 71 (1 d), MiCAr.
[156] Art 71 (1), subpara 2, MiCAr.

purchasers[157]. Furthermore, in order to maintain and operate an effective policy on conflicts of interest referred to in Article 65 CASPs «shall have specific and adequate procedures in place to prevent, monitor, manage and potentially disclose any conflicts of interest»[158] that can occur:

a. If «the crypto-asset service providers place the crypto-assets with their own clients»[159];
b. If «the proposed price for placing crypto-assets has been overestimated or underestimated»[160].

The sixth category of obligations for CASPs regards the service of the **reception and transmission of orders on behalf of third parties**. When a client gives an order to sell or buy a crypto-asset, the CASP in turn takes that order and transmits it to another CASP for the execution of that order. This second CASP, however, must have the authorization for one or more of these services:

- the execution of orders for crypto-operation of a trading platform for crypto-assets;
- the operation of a trading platform for crypto-asset;
- the exchange of crypto-assets against official currencies or other crypto-assets[161].

MiCA regulation states that in order to fulfil properly this kind of service, CASPs «shall establish and implement procedures and arrangements which provide for the prompt and proper transmission of client's orders for execution on a trading platform for crypto-assets or to another crypto-asset service provider»[162]. Furthermore, CASPs «shall not receive any remuneration, discount or non-monetary benefit for routing clients' orders received from clients to a particular trading platform for crypto-assets or to another crypto- asset service provider»[163].

MiCAr also establishes another obligation for CASPs that offer the service of the reception and transmission of orders on behalf of third parties. In fact, in Article 72 it is

[157] *Ibid.*
[158] Art 71 (2), MiCAr.
[159] Art 71 (2 a), MiCAr.
[160] Art 71 (2 b), MiCAr
[161] On this particular matter see Article 3 (1), (16), MiCAr.
[162] Art 72 (1), MiCAr.
[163] Art 72 (2), MiCAr.

stated that those CASPs «shall not misuse information relating to pending clients' orders and shall take all reasonable steps to prevent the misuse of such information»[164].

The *ratio* behind these obligations is to avoid hidden fee structures, conflicts of interest and kick-back arrangements between the two CASPs and, also, to promote the obligation of CASPs to act in the best interest of their clients[165].

The seventh and last category of obligations established for CASPs refers to the one regarding the service of the **advice on crypto-assets**. MiCA regulation has sought to ensure that this service is given to clients by CASPs that have a sufficient expertise on the topic the advice is given to. This is the reason why CASPs asking to be authorized to provide to give advice on crypto-assets must demonstrate[166] in their application that the people who give advice on behalf of the applicant have the necessary experience and knowledge in order to fulfil their obligations[167].

Furthermore, Article 73 states that CASPs «shall assess the compatibility of such crypto-assets with the needs of the clients and recommend them only when this is in the interest of the clients». Moreover, CASPs providing advice on crypto-assets must also «request information about the client or prospective client's knowledge of, and experience in crypto-assets, objectives, financial situation including the ability to bear losses and a basic understanding of risks involved in purchasing crypto-assets»[168].

It is also necessary that CASPs «establish, maintain and implement policies and procedures to enable them to collect and assess all information necessary to conduct this assessment for each client. They shall take reasonable steps to ensure that the information collected about their clients or prospective clients is reliable»[169]. In addition to this, Article 73 states that this assessment shall take place on an ongoing basis, at least every two years for each client after the initial assessment[170].

Article 73 goes on stating that CASPs must provide its clients with a report on that assessment that summarize both the client's demands and needs and the advice given[171].

[164] Art 72 (3), MiCAr.
[165] On this particular matter, see Art 59 (1), MiCAr.
[166] On this particular matter, see Art 54 (2 r), MiCAr.
[167] Art 73 (2), Recital 63, MiCAr.
[168] Art 73 (3), MiCAr.
[169] Art 73 (4), MiCAr.
[170] Art 73 (6), MiCAr.
[171] Art 73 (7), Recital 63, MiCAr.

Where clients do not provide the requested information or where CASPs come to the conclusion that their client has insufficient knowledge, « crypto-asset service providers that are authorised to provide advice on crypto-assets shall inform those clients or prospective clients that the crypto-assets or crypto-asset services may be inappropriate for them and issue them a warning on the risks associated with crypto- assets. That risk warning shall clearly state the risk of losing the entirety of the money invested or converted into crypto-assets. Clients shall expressly acknowledge that they have received and understood the warning issued by the crypto-asset service provider concerned»[172]. Either way, CASPs that offer advice on crypto-asset must always warn their clients that due to their tradability, the value of crypto-assets may fluctuate[173].

CASPs that provide advice on crypto-assets, however – as opposed to the corresponding provision of MiFID II on investment advice – are not obliged to disclose the cost of the advice to their potential clients[174].

1.5. Brief summary on CASP's functioning

To sum up, it is common ground that the crypto-asset services of MiCAr are predominantly inspired by the investment activities defined by the MiFID II. Only the services regarding the administration and of crypto-assets for the sake of third parties are excluded due to the fact that DLT poses very specific issues to users. That is why, pursuant to MiCA regulation, portfolio management should not be a crypto-asset service whatsoever; thus, anyone seeking to provide crypto-assets services must first seek authorization as such. In fact, only legal entities with a registered office in the EU are qualified to be authorized as a CASP. However, authorization is only given for those specific services for which the requesting CASP has asked to be authorized and for which it is possible to demonstrated that it adheres to the MiCA regulation provisions.

[172] Art 73 (5), MiCAr.
[173] *Ibid.*
[174] On this particular matter, see Art 24 (4 c) MiFID II; Recital 72 MiFID II and Art 59 (4), MiCAr.

2. What could change in practice for the Issuers

2.1. Issuers Introduction

As done for the CASP, the MiCA regulation also tries to maintain the same approach in harmonizing the figure of the crypto-asset issuer, even if this role is much more technology-used specific than the CASPs: therefore, defining unique guidelines and parameters to detect the role of the issuer may not be straightforward, as we will see in Chapter 3 for the issuer-less crypto-assets.

The definition of "*Issuer*" given by the MiCAr is the following:
«'issuer of crypto-assets' means a 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-assets»[175].

Multiple interesting points are worth noting:

- Even though no direct definition is given for the verb used "*to issue [a crypto-asset]*", it can be indirectly deducted by the definition of the issuer. It's no secret that the approach used by Commission in addressing the role of the issuer is inspired by the approach used in the Prospectus Regulation (2017/1129)[176];
- In relation to the previous point, MiCAr although specifies the meaning of "*offer to the public*" on the point 7 of the same Article 3.
  The point states:
  «'offer to the public' means an offer to third parties to acquire a crypto-asset in exchange for fiat currency or other crypto-assets»[177], which it basically refers to the first sale of the crypto-asset (or better, the used technology underlying) after its creation.

As we will see, simply defining the issuer as the "*crypto-asset creator*" would have been, other than reductive, also wrong, as there are specific cases in which the issuer cannot be determined or the real issuer of the item is not the physical creator of the asset.

[175] Art 3 (6), MiCAr.
[176] Art 2 (h), Prospectus Regulation (n. 2017/1129).
[177] Art 3 (7), MiCAr.

Therefore, in order to avoid any problems of lack of regulation, due to the fact that *dummy-creators* would have been used, the MiCAr regulates the people responsible for the crypto-asset entrance into the market: how? As seen above, the formula used is combining the people responsible for the first sale of the item (as an approximation, usually the physical item creators) with the people responsible for contacting the CASP to gain access to the platforms. As we can see, the general approach of generic, but at the same time comprehensive, targeting is used also in this case.

The reason of indirect addressing of the material creator of the crypto-asset can easily be understood by analyzing the process from the risk perspective: by regulating the and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender. entrance into the market, the Commission addressed the risk of inappropriate issuance of crypto-assets, as the entrance into the market is a crucial, and necessary, point of every asset. With this approach, the Commission effectively posed obligations in order to prevent possible inappropriate issuance, avoiding the problem of applicability to the issuer definition.

The issuer category have been divided into three subgroups, each address by specific Titles of the MiCAr.

These groups have been clustered based on the nature of the crypto-asset issued:

- **ART** (Asset Referenced Tokens): like the name, ART are a type of crypto-asset of which its value is determined – as well as influenced – by another, usually physical, asset (fiat currencies or commodities).

  The definition of ART given by the MiCAr is: «'asset-referenced token' means 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»[178];

  The link between a crypto-asset and a physical commodity may not be immediate, but a useful example, in order to have a better understanding of the phenomenon, would be the Tether Gold: in fact, the Tether Gold asset value is backed by gold

[178] Art 3 (3), MiCAr.

stored in a vault in Switzerland. The customers are so indirectly buying gold, and that's explains the linkage between values[179].

The ART most famous example is, however, the Diem token (formerly known as Libra Project), which was a token issued by Facebook/Meta, influenced by a basket of real-world currencies, with the purpose of being used as a cross-border world currency. Due to budget constraints and legislation uncertainties, it was shut down on January 2022[180].

- **EMT** (Electronic Money Tokens): a type of crypto-asset the main purpose of which is to be used as a means of exchange. Usually, due to its usage, the E-money tokens are also "*stablecoins*", meaning that they maintain a relative stable value in time like a fiat currency.

  The definition given by the MiCAr is in fact: «'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»[181]

- **Neither ART nor EMT**: a special *catch-all* category containing every item not falling into the previous two subgroups. The importance of such category is crucial: in fact, this category is granting the full regulation of the entire crypto-asset landscape.

With the same CASP approach, the NCAs highlighted by each Member State will be responsible for the supervision the issuers based in their territory: this is possible only for those who meet the requirement of being a legal person.

In addition, one of the most important provisions of the issuer is the mandatory publication of an informative document (referred to as "*White Paper*"), showing the crypto-asset characteristics, technology, usages, risks and other technical information.

[179] On this particular matter, see the following link: https://gold.tether.to/ .

[180] On this particular matter, see LAWYER L., (2022), *Asset-Referenced Tokens Under the EU's Proposed Markets in Crypto Assets Regulation*, electronically available at *Medium*: https://medium.com/coinmonks/asset-referenced-tokens-under-the-eus-proposed-markets-in-crypto-assets-regulation-458c317577bb#:~:text=Under%20MiCA%2C%20a%20crypto%2Dasset,a%20combination%20of%20such%20assets%E2%80%9D.

[181] Art 3 (4), MiCAr.

2.2. Issuers of Asset Referenced Tokens

As anticipated, the Asset Referenced Tokens represent a consistent portion of the crypto-asset landscape, and the market's tendency in the medium-long term is to further invest in such technology, as the final customers (but also the regulating/supervising entities, such as the ECB) want assets with a pretty stable value over time. As the crypto-assets nowadays maintain a considerable volatility (due to multiple causes), backing them with stable-value commodities/fiat currencies seems the perfect combination, combining the financial stability given by the underlying asset with the possibilities given by the DLT technology of the crypto-asset itself.

For such reasons, the Commission gave a high degree of importance in formalizing the Title III of the MiCA regulation – composed by 6 Chapters and 28 articles – regulating the risks arising on the issuer-side.

The regulatory approach is quite simple and, as we will see in the following paragraphs, it is shared between ART, EMT and "catch-all" category, even if in this particular case, due to the high degree of specific risk given by the popularity of the category, the requirements are by far more stringent than in the other categories.

The first two requirements are fundamental:

- The ART issuer must be a legal entity with a registered office in an EU Member State[182]. It must be noted that here we have the first difference with the "catch-all" category, as in its requirement is not specified that the legal entity must be placed in an EU Member State. The reason behind this difference is explained in the following point;
- The ART issuer must be formally authorized by the NCA of the Member State in which the office is registered.

  The point 1 of the Article 15 in fact states that «no issuer of asset-referenced tokens shall, within the Union, offer such tokens to the public, or seek an admission of such assets to trading on a trading platform for crypto-assets, unless such issuers have been authorized to do so in accordance with Article 19 by the competent authority of their home Member State»[183]. The location requirement of

[182] Art 15 (2), MiCAr.
[183] Art 15 (1), MiCAr.

the previous point is, therefore, necessary to give NCAs the power to regulate the entrance into the market by an authorization process.

On this point, some exemptions are present, but they all share a risk-based criteria: the Commission set a threshold of 5 million euros (within 12 months) under which the issuer are not required to be approved by the NCA. The "White Paper" producing requirement is still present.

Not only the ART entrance into the market is formally authorized by NCAs, but also the "White Paper" is mandatory (in form and contents) and must be approved as well. How we'll see, the "catch-all" category is not required to do so.

Another worth mentioning point in relation to authorization exception is about the Credit Institutions group, issuing their ART.

The Article 2, point 4, in fact states that: «where issuing asset-referenced tokens, including significant asset-referenced tokens, credit institutions authorised under Directive 2013/36/EU shall not be subject to:

(a) the provisions of chapter I of Title III, except Articles 21 and 22;

(b) Article 31»[184].

The Commission objective here is simple: as the ART are the most popular category of crypto-asset in big financial institution, the regulation does not want to block/slow down the business implementations of such technology. It is in fact the exact opposite as the Commission, already in the draft version of the regulation, is eliminating some burocracy, always having in mind a risk-based approach. In fact, Credit Institutions already authorized to operate on the EU financial markets are already complying with heavy entity-level requirements, so that specific crypto-product authorization won't add a significant assurance on the underlying risks.

Interesting to see that Credit Institutions already authorized are completely excluded by the applicability of the Title III, except for three articles:

- Article 21, which sets requirements on the modifications to the white papers[185];

[184] Art 2 (4), MiCAr.
[185] Art 21, MiCAr.

- Article 22, which sets liabilities for the information published on the white papers[186];
- Article 31, which sets specific crypto-asset funds requirements (to be added to the funds requirements of the Credit Institution business)[187];

It also must be noted that the first two articles regulate the white papers, setting requirements for the modifications and specifying the liabilities: the curious fact is that, technically speaking, the Credit Institutions exclusion from Title III also exclude them by the white paper publishing requirements.

It is now unclear if it's an error or a wanted specific piece of regulation, but the more probable answer seems the error, as the point 28 specifically states out the Credit Institutions requirement to produce white papers: «Offers to the public of asset-referenced tokens in the Union or seeking an admission of such crypto-assets to trading on a trading platform for crypto-assets should be possible only where the competent authority has authorised the issuer of such crypto-assets and approved the crypto-asset white paper regarding such crypto-assets. The authorisation requirement should however not apply where the asset-referenced tokens are only offered to qualified investors, or when the offer to the public of asset-referenced tokens is below a certain threshold. Credit institutions authorised under Directive 412013/36/EU of the European Parliament and of the Council should not need another authorisation under this Regulation in order to issue asset-referenced tokens. In those cases, the issuer of such asset-referenced tokens should be still required to produce a crypto-asset white paper to inform buyers about the characteristics and risks of such asset-referenced tokens and to notify it to the relevant competent authority, before publication»[188].

Before briefly analyzing the other ART Issuer requirements, worth mentioning is the Article 36, surely short but extremely important in order to understand the Commission approach to the ART regulation.

[186] Art 22, MiCAr.
[187] Art 31, MiCAr.
[188] Recital 28, p. 21, MiCAr.

The Article in question states that «Issuers of asset-referenced tokens or crypto-asset service providers shall not provide for or any other benefit related to the length of time during which a holder of asset-tokens holds asset-referenced assets»[189].
Here we can see the Commission's will in maintaining the ART crypto-assets not a store-of-value but instead a technology used for short-medium term exchanges. This Article will be one of the toughest to be complied with, as often the trading platforms (as this specific Article is applicable to issuers but also to CASP) provide interest-like bonuses.

In order to preserve the Market Integrity, but also the general monetary stability, it is understandable that the Commission does not want to further incentive long-term investments on a technology which the general public is not yet fully informed about.

As said, the Issuers' main role is placed at the beginning of a crypto-asset life, even if they may not be the physical asset creators, they are responsible for its entrance into the market.

Given the specification of "*Issuer does not mean creator*", the Commission therefore cannot regulate **how** the assets are physically produced via coding. What the Commission can do is to regulate the "behavior" of the asset after the public release, as we well as the information provided to the customers: as already said in the previous chapters, the MiCA regulation approach is highly oriented to the customer protection.

The recital 32 introduces exactly this issue: «To ensure consumer protection, issuers of asset-referenced tokens should always act honestly, fairly and professionally and in the best interest of the holders of asset-referenced tokens. Issuers of asset-referenced tokens should also put in place a clear procedure for handling the complaints received from the holders of crypto-assets»[190].

The main challenge is the objectivity of such principle: how can the Commission tell if the issuers are acting "honestly, fairly and professionally"?

The recital mentioned above is only one general, introductory principle, but it did not remain unaddressed. This is why Article 23 formalizes exactly what was laid down as a principle, even if the objectivity still remains an issue: «Issuers of asset-referenced tokens shall:
(a) act honestly, fairly and professionally;

[189] Art 36, MiCAr.
[190] Recital 32, p. 22, MiCAr.

(b) communicate with the holders of asset-referenced tokens in a fair, clear and not misleading manner»[191].

It is interesting to notice the stress put on point B and, in particular, all the attention given to how the information/communications are spread (more in details, it is referred primarily to the white papers release).

As we have already seen, here it is visible that not only the general rules of conduct but also the marketing communications are integrated as well.

Article 25 (point 1) formalizes exactly the 4 principles on which the marketing communications are based on:

«*Any marketing communications relating to an offer to the public of asset-referenced tokens, or to the admission of such asset-referenced tokens to trading on a trading platform for crypto-assets, shall comply with all of the following:*

(a) the marketing communications shall be clearly identifiable as such;

(b) the information in the marketing communications shall be fair, clear and not misleading;

(c) the information in the marketing communications shall be consistent with the information in the crypto-asset white paper;

(d) the marketing communications shall clearly state that a crypto-asset white paper has been published and indicate the address of the website of the issuer of the crypto-assets»[192].

The first two points are related to the provisions for the general communications to the public, even if the common problem of objectivity still remains. The Commission, in order to address the matter, formalized the following two points (C and D), with a simple but extremely effective method: as directly reviewing every communication made by the issuers to the customers would be impractical, the principle basically states that the communications have to be made in accordance with the white paper, correctly approved and published.

As anticipated, and as we will see in the following paragraphs, the white paper is one of the central points MiCAr is based on: the Commission has designed the process that the NCAs have to follow in order to approve the white paper, and the following

[191] Art 23, MiCAr.
[192] Art 25 (1), MiCAr.

communications must be aligned to it. In this way, even if not directly, the NCAs define the guidelines for all the issuers communications to the public.

These are not the only principles related to communications because the Commission also sets provisions for a continuous update to the customers, especially for the disclosure of the current status of the assets and issuer funds[193].

Before analyzing the provisions related to the white paper formalization, it is important to briefly mention the other provisions made by the Commission for the ART issuers.

The most notable areas treated are: Corporate Governance, Complaints Management, Conflicts of Interests, Reserve of Assets, Changes to the business model.

- **Corporate Governance**: addressed by the comprehensive Article 30, it lays down the requirements, in a Corporate Governance perspective, that the issuers of ART have to comply with[194]. The key point mentioned by such articles is a clear and organized management structure, which has to be composed by high specialized professionals (in terms of competences, qualifications, experience, skills, reputation, ethics).

  Even though it may seem obvious, the point 4 of the Article it is worth mentioning because it reflects the anti-money-laundering and anti-terrorism purposes of the MiCA regulation: «None of the persons referred to in paragraphs 2 or 3 shall have been convicted of offences relating to money laundering or terrorist financing or other financial crimes»[195].

- **Complaints Management**: addressed by the Article 27, the provisions here formalized are related to complaints management as well as customer-care services[196]. The first and fourth points of the Article give us what can be easily defined as the best summary of the MiCAr approach, as well as let us notice once more how much the regulation is customer-protection oriented:

- **Point 1** «Issuers of asset-referenced tokens shall establish and maintain effective and transparent procedures for the prompt, fair and consistent handling of complaints received from holders of asset-referenced tokens. Where the asset-referenced tokens

[193] Art 26, MiCAr.
[194] Art 26, MiCAr.
[195] Art 30 (4), MiCAr.
[196] Art 27, MiCAr

are distributed, totally or partially, by third-party entities as referred to in Article 30(5) point (h), issuers of asset-referenced tokens shall establish procedures to facilitate the handling of such complaints between holders of asset-referenced tokens and such third-party entities»[197].

- **Point 4** «Issuers of asset-referenced tokens shall investigate all complaints in a timely and fair manner and communicate the outcome of such investigations to the holders of their asset-referenced tokens within a reasonable period of time»[198].

- **Conflicts of Interests**: formalized in the Article 28, the conflict of interests addresses the risks of people potentially influencing the crypto-asset behavior via fraudulent Management decisions[199].

  The principles, on which the conflict of interests prevention is based on, are mainly two:

- users with potential high influences disclosure;
- timely detection of potential conflicts.

  In particular, the **first point** of the Article states: «*Issuers of asset-referenced tokens shall maintain and implement effective policies and procedures to prevent, identify, manage and disclose conflicts of interest between themselves and:*

  (a) their shareholders;

  (b) the members of their management body;

  (c) their employees;

  (d) any natural persons who either own, directly or indirectly, more than 20% of the asset-backed crypto-asset issuer's share capital or voting rights, or who exercise, by any other means, a power of control over the said issuer;

  (e) the holders of asset-referenced tokens;

  (f) any third party providing one of the functions as referred in Article 30(5), point (h);

  (g) where applicable, any legal or natural persons referred to in Article 35(3). Issuers of asset-referenced tokens shall, in particular, take all appropriate steps

[197] Art 27 (1), MiCAr.
[198] Art 27 (4), MiCAr.
[199] Art 28, MiCAr.

to prevent, identify, manage and disclose conflicts of interest arising from the management and investment of the reserve assets referred to in Article 32»[200].

- **<u>Reserve of Assets</u>**: this one is introduced by the Article 31, which sets the requirements for own funds in a prudential perspective (aligned with the approach already used for the Credit Institutions)[201]. The issue in question is extensively addressed by the chapter 3, which is composed by multiple articles:

- **Article 32**: such Article, in combination with the previous one, sets the requirements for the issuers to constitute and maintain, at all times, reserves of assets[202], one for each crypto-asset issued to the public[203]. In a prudential perspective, it is worth noting the usage of «prudential management of the reserve assets» in the point 3[204].
- **Article 33:** such Article sets the provisions for the formal maintenance and custody of the reserves[205].
- **Article 34:** such Article defines the provisions for the investments of the reserves. In a prudential perspective, in fact, the reserves of assets can be financially invested, but only in highly liquid financial instruments with minimal market and credit risk[206]. This is why, to prevent any possible risk related to funds disposal, the investments have to be able to be liquidated quickly, without significant influence on the value[207].
- **Article 35:** such Article defines the obligation by the issuers to define the rights of the crypto-assets holders on the reserves. This Article is extremely important because the function of the reserves is, in fact, to protect the customers from the risks of possessing the crypto-asset[208].
- **Article 36:** we have already mentioned the Article 36 before analyzing in details the provisions set. Such Article is related to the prohibition of interests/benefit issuance by the issuers to the holders of crypto-assets[209].

[200] Art 28 (1), MiCAr.
[201] Art 31, MiCAr.
[202] Art 32 (especially point 1), MiCAr.
[203] Art 32 (2), MiCAr.
[204] Art 32 (3), MiCAr
[205] Art 33, MiCAr.
[206] Art 34, MiCAr.
[207] *Ibid.*, first comma.
[208] Art 35, MiCAr.
[209] Art 36, MiCAr.

- **<u>Changes to the business model</u>**: such issue is heavily related to the white paper issuance, as the Article addressing this point is the 21. The latter Article defines, in fact, the provisions for the issuers, already authorized[210] (authorization with comprehend the authorization of the white paper, Article 19), modifying their business model[211].

  The first point states that: «*Issuers of asset-referenced tokens shall also notify the competent authority of their home Member States of* ***any intended change of the issuer's business model likely to have a significant influence on the purchase decision of any actual or potential holder of asset-referenced tokens****, which occurs after the authorisation mentioned in Article 19. Such changes include, among others, any material modifications to:*

  (a) the governance arrangements;

  (b) the reserve assets and the custody of the reserve assets;

  (c) the rights granted to the holders of asset-referenced tokens;

  (d) the mechanism through which asset-referenced tokens are issued, created and destroyed;

  (e) the protocols for validating the transactions in asset-referenced tokens;

  (f) the functioning of the issuer's proprietary DLT, where the asset-referenced tokens are issued, transferred and stored on such a DLT;

  (g) the mechanisms to ensure the redemption of the asset-referenced tokens or to ensure their liquidity;

  (h) the arrangements with third parties, including for managing the reserve assets and the investment of the reserve, the custody of reserve assets, and, where applicable, the distribution of the asset-referenced tokens to the public;

  (i) the liquidity management policy for issuers of significant asset-referenced tokens;

  (j) the complaint handling procedure»[212].

  It is now clear that every modification listed in the first point must be notified to the NCA, and therefore approved: every modification must be traced in the white paper, which is the ultimate informative document.

[210] Art 19, MiCAr.
[211] Art 21, MiCAr.
[212] Art 21 (1), MiCAr.

This links us to the final important area regulated for the ART issuers, which will be briefly analyzed in the following paragraph.

As mentioned before, the white paper is an informative document formalized by the issuer with the aim of describing itself, the participants involved[213], as well as the type of the crypto-asset issued and offered to the public[214].

It must be noted that the characteristics mentioned above are from the Article 5, formally in the Title II dedicated to the issuers "*other than asset-referenced tokens or e-money tokens*" (the catch-all category), a group which will be described in a following dedicated paragraph.

Even if the white paper provisions seem to be only for the catch-all category Title, they are valid also for the ART issuer, and the reason is simple: the Commission approach consisted in defining all the basic provisions for the catch-all category (the less regulated one), and then adding the necessary provisions on the top for the ART and EMT.

For this reason, the articles valid for the ART issuers related to the white papers are:

- **Article 4:** Article in common for all the three categories (ART, EMC and catch-all), defining the entities required to produce a white paper[215];
- **Article 5:** Article in common for all the three categories (ART, EMC and catch-all), defining the information required to be disclosed in a white paper[216];
- **Article 7**: Article in common for all the three categories (ART, EMC and catch-all), defining the parameters to correctly notify the white paper;[217]
- **Article 16**: this is probably the most important Article as well as the following one, as it explicitly links the previous articles (formally only for the catch-all category) to the ART category. In particular, the point 2 clearly defines the requirements for ART issuers to draft a white paper[218];

[213] Art 5 (1 a), MiCAr.
[214] Art 5 (1 b), MiCAr.
[215] Art 4, MiCAr.
[216] Art 5, MiCAr.
[217] Art 7, MiCAr.
[218] Art 16 (2i), MiCAr.

- **Article 17**: this Article specifies the information required to be inserted in the ART white paper **in addition** to the one already specified in the Article 4, hence repeating once more its applicability also to the ART category[219].

[219] Art 17, MiCAr.

For explanatory purposes, please see the following attached summary of Aurus tokens' white paper[220]:

Contents

[220] AURUS, *Aurus token white paper*, electronically available at: https://aurus.io/aurus-whitepaper.pdf.

2.3. Issuers of Electronic Money Tokens

As mentioned before, the ART as well as the Electronic Money Tokens represent a consistent percentage of the crypto-asset capitalization in the market, but most importantly, they have specific characteristics that need to be addressed.
Moreover, due to the specific usage of such tokens, it is probably the category that is more destined to see the major growth in the near future.

For such reasons, the Commission formalizes an entire Title (Title IV) of the MiCA regulation, and even if it is relatively short (because it is, in fact, only composed by 2 chapters and 10 articles) it addresses specific risks arising on the issuer-side. By the length of the Title, we can observe how the Commission is prudentially waiting for the EMTs to fully develop, addressing now only the major and crucial risks.

The main difference between EMT and ART issuers which can be initially noted lays in the authorization process. In fact, if the ART issuers require to be authorized by a NCA of a EU Member State[221] – as it is as written in the point 1 of the Article 15 – the EMT issuers have to be authorized not by a NCA of a Member State, but rather by an "Electronic Money Institution" in accordance with the EMD2[222].

Therefore, it is an indirect regulation by MiCAr, as the Commission is explicitly using the EMD as a proxy: the main advantage is that, once the EMD and MiCAr

[221] Art 15 (1), MiCAr.
[222] Art 2 (1), EMD2.

compatibility had been assessed, there is no need to further regulate the EMT authorization and this entails a consistent time saving. However, this huge advantage is also the main disadvantage: *de-facto*, the MiCAr approach in regulating the EMT issuers (especially in the authorization subprocess) is EMD2-dependant. Also worth mentioning: the MiCAr is an EU regulation, meanwhile the EMD2 is a directive, with all the slight adoption differences between EU member states. The Commission approach, however, is crystal-clear: for the moment, considering also the specific category, the MiCA regulation will only add specific parts, completing the EMD2, which already address relevant risks, as the issuer correct authorization.

The specific Article, which at first sight can be misleading, is the Article 43 which states:

«*No electronic money tokens shall be offered to the public in the Union or shall be admitted to trading on a trading platform for crypto-assets unless the issuer of such electronic money tokens:*

(a) is authorised as a credit institution or as an 'electronic money institution' within the meaning of Article 2(1) of Directive 2009/110/EC;

(b) complies with requirements applying to electronic money institution set out in Titles II and III of Directive 2009/110/EC, unless stated otherwise in this Title;

(c) publishes a crypto-asset white paper notified to the competent authority, in accordance with Article 46.

For the purpose of point (a), an 'electronic money institution' as defined in Article 2(1) of Directive 2009/110/EC shall be authorised to issue 'e-money tokens' and e-money tokens shall be deemed to be 'electronic money' as defined in Article 2(2) of Directive 2009/110/EC.

An e-money token which references a Union currency shall be deemed to be offered to the public in the Union»[223].

The interesting point in the authorization Article, other than the already discussed point (a), is the point (c): in fact, it is a clear example of the "*add-on approach*" by the Commission, as even if the issuer has to be authorized in accordance with the EMD2, it has to present a white paper, following the same principles laid down for the ART

[223] Art 43, MiCAr.

category. With this provision, the Commission aims to prevent relevant differences in the various crypto-assets categories: the only differences will depend on specific characteristics of the assets.

Another main characteristic for the EMT issuers is the required funds of at least 350.000 euros in order to receive the initial approval[224]. In addition, to be authorized to operate in the market, the fund requirement is set to be 2% of the current value of the token circulating in the market[225]. It must be noted the prudential approach of MiCAr in relation to the customer protection principles: the point 5 of the Article 5 of the EMD2, in fact, leaves the possibility to the authorities to demand a consistent raise of such percentage.

The extract from the Article is reported below: «*On the basis of an evaluation of the risk-management processes, of the risk loss databases and internal control mechanisms of the electronic money institution, the competent authorities may require the electronic money institution to hold an amount of own funds which is up to 20 % higher than the amount which would result from the application of the relevant method in accordance with paragraph 2, or permit the electronic money institution to hold an amount of own funds which is up to 20 % lower than the amount which would result from the application of the relevant method in accordance with paragraph 2*» [226].

Even though it is clear that such provisions are set in EMD2, and not in the MiCAr, and at a first glance the fund requirements seems to be an unaddressed point, the Commission fully refers to the EMD2 articles reported above in the Article 43 (1b) which simply states that:

«*No electronic money tokens shall be offered to the public in the Union or shall be admitted to trading on a trading platform for crypto-assets unless the issuer of such electronic money tokens:*

(a) […]

(b) complies with requirements applying to electronic money institution set out in Titles II and III of Directive 2009/110/EC, unless stated otherwise in this Title»[227].

[224] Art 4, EMD2.
[225] Art 5 (1)(2)(3), EMD2.
[226] Art 5 (5), EMD2.
[227] Art 43 (1b), MiCAr.

At this point, a comparison between these provisions and the corresponding obligations for issuers of the ART category clearly attests that the Commission used the EMD2 as a reference not only for the EMT category (which a good portion of the provisions is simply a direct referral) but also for the ART category.

With the purpose of not completely blocking the EMT market with excessive formal steps, the Commission also set exceptions, always with an upper value limit of the outstanding asset in the market, more precisely consisting in 5 million Euros over a period of 12 months[228]. In other words, the Commission is setting a small lap time in with the issuers do not have to request for the authorization and, more importantly, reserve some funds: this provision is clearly facilitating the publishing of new, emerging, EMT.

The last main topic of the EMT regulation is the white paper requirement. As previously highlighted, the difference with the ART category is quite substantial: while for the ART category not only the white paper publishing is mandatory, but also it has to be approved by the NCA [as seen in the previous sub-chapter, at the Article 16(2i)], for the EMT's only the publishing, and not the formal approval, of the white paper is required[229], as this specific provision is missing in the related Article 46, which states that: «*Before offering e-money tokens to the public in the EU or seeking an admission of such e-money tokens to trading on a trading platform, the issuer of e-money tokens shall publish a crypto-asset white paper on its website*» [230].

Practically, the information detailed in the ART White papers and in the EMT White papers are substantially the same: therefore, the table of contents for the Aurus token (the example mentioned in the paragraph regarding the ART category) could be applied, for explanatory purposes, also for the EMT category.

[228] Art 43 (2), MiCAr.
[229] Art 43 (1c), MiCAr.
[230] Art 46 (1), MiCAr.

2.4. Issuers of Crypto-Assets different from ART and EMT

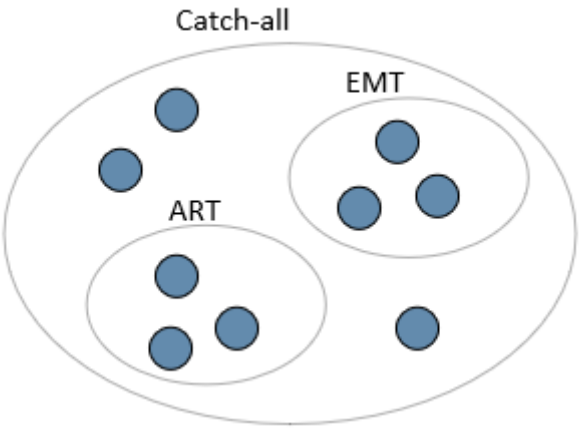
This broad category, regulated in the Title II of the MiCA regulation, addresses the possible gaps in the legislation described above.

As already explained, the third catch-all category is necessary due to the nature of the previous two categories (ART and EMT): in order to be addressed by one of such categories, the items must reflect specific characteristics, and the option of both ART and EMT non-applicability is more than possible, considering also the items population and variety.

In fact, the aim of such catch-all category is dual:

1) Prevent empty gaps of unregulation, due to non-applicability of ART and EMT specific provisions;
2) Setting up a base regulatory layer, on which various provisions for specific (emerging) technology could be added.

For simplicity purposes, the category is being explained after the ART and EMT ones: all the major points have been already described in the previous two sub-chapters, as the provisions of this category are used also for the ART and EMT, but not vice-versa.



Starting with the authorization criteria, there are no other feasible alternatives than the ones provided by the Article 4:

«*No issuer of crypto-assets, other than asset-referenced tokens or e-money tokens, shall, in the Union, offer such crypto-assets to the public, or seek an admission of such crypto-assets to trading on a trading platform for crypto-assets, unless that issuer:*

(a) is a legal entity;

(b) has drafted a crypto-asset white paper in respect of those crypto-assets in accordance with Article 5;

(c) has notified that crypto-asset white paper in accordance with Article 7;

(d) has published the crypto-asset white paper in accordance with Article 8;

(e) complies with the requirements laid down in Article 13»[231].

As already mentioned in the requirements for the white paper for the ART category, this Article provides the basic guidelines for the admission of an issuer of items not falling into ART and EMT categories. It must be noted that such article does not consider the nature of the technology (due to the variety of the catch-all category): it would not be feasible to define every possible technology type, nor try to clusterize them, as possible regulatory gaps may occur because it would jeopardize the final objective of this broad category.

The point 2 of the same article is curious but at the same time coherent with the MiCAr general approach of not harming and preventing the development of the crypto-sector: in fact, it poses specific exclusions to the white paper requirements (always with a risk-based approach):

«*Paragraph 1, points (b) to (d) shall not apply where:*

(a) the crypto-assets are offered for free;

(b) the crypto-assets are automatically created through mining as a reward for the maintenance of the DLT or the validation of transactions;

(c) the crypto-assets are unique and not fungible with other crypto-assets;

(d) the crypto-assets are offered to fewer than 150 natural or legal persons per Member State where such persons are acting on their own account;

(e) over a period of 12 months, the total consideration of an offer to the public of crypto-assets in the Union does not exceed EUR 1 000 000, or the equivalent amount in another currency or in crypto-assets;

(f) the offer to the public of the crypto-assets is solely addressed to qualified investors and the crypto-assets can only be held by such qualified investors.

For the purpose of point (a), crypto-assets shall not be considered to be offered for free where purchasers are required to provide or to undertake to provide personal data to the

[231] Art 4 (1), MiCAr.

issuer in exchange for those crypto-assets, or where the issuer of those crypto-assets receives from the prospective holders of those crypto-assets any third party fees, commissions, monetary benefits or non-monetary benefits in exchange for those crypto-assets» [232].

Regarding the practical contents of the white paper, if required, they are the same of the ones already described for the ART category, as defined by Article 5.

Other general provisions in the Title II are referred to the marketing communications even in relation to the customer protection. Such provisions will be briefly described in the following sub-chapter.

3. What could change in practice for the Financial Customers

Even if the customer category is not directly addressed with a dedicated Title, various Articles focus on the customers as the main beneficiary of the regulations. As already said before, the MiCAr regulatory approach is highly customer-protection oriented, meaning that the regulatory framework addresses mostly the potential risks affecting the end customers rather than the potential risks arising from this category and its usage of the crypto-assets.

Due to the lack of a dedicated Title, the most relevant articles displaying the customer protection approach are the following:

a) <u>For the Issuers category</u>:

- Article 6: provision regulating the marketing communications, determining the guidelines which must be followed in communicating the offering of a crypto-asset to the public. In particular, the Article states that «*Any marketing communications relating to an offer to the public of crypto-assets, other than asset-referenced tokens or e-money tokens, or to the admission of such crypto-assets to trading on a trading platform for crypto-assets, shall comply with all of the following:*
(a) the marketing communications shall be clearly identifiable as such;

[232] Art 4 (2), MiCAr.

(b) the information in the marketing communications shall be fair, clear and not misleading;

(c) the information in the marketing communications shall be consistent with the information in the crypto-asset white paper, where such a crypto-asset white paper is required in accordance with Article 4;

(d) the marketing communications shall clearly state that a crypto-asset white paper has been published and indicate the address of the website of the issuer of the crypto-assets concerned». One noticeable characteristic is that this Article is pretty heterogeneous in the level of details used: while points A, B and C are quite generic, the point D explicitly states that not only the communications should reflect the information reported in the white paper, but it is also stated that every communication must indicate the website of the issuer. The aim is probably to prevent any fraudulent and/or misleading communication to the customers.

- **Article 7:** this Article, at subpoint (2), defines the timing requirements for notifications to the NCA related to marketing communications. In particular it states that: «*Issuers of crypto-assets, other than asset-referenced tokens or e-money tokens, shall notify their crypto-asset white paper, and, in case of marketing communications as referred to in Article 6, such marketing communications, to the competent authority of their home Member State at least 20 working days before publication of the crypto-asset white paper. That competent authority may exercise the powers laid down in Article 82(1)*»[233]. This time requirement is truly fundamental as it leaves the NCA enough time to prevent any misleading communication to the public by fraudulent issuers.

The Article also mentions the Article 82 regarding the power of the competent authorities. The Article 82, in fact, states at point 1.G: «*to suspend, or to require a crypto-asset service provider to suspend the provision of crypto-asset services where the competent authorities consider that the crypto-asset service provider's situation is such that the provision of the crypto-asset service would be detrimental to consumers' interests*»[234]. This is one of the clearest examples of the customer protection approach held by the Commission.

[233] Art 7 (2), MiCAr.
[234] Art 82 (1g), MiCAr.

- **Article 8:** the issuer website continues to have a central role in authenticating the information disclosed in the white paper and/or marketing communications. That is why, «*Issuers of crypto-assets, other than asset-referenced tokens or e-money tokens, shall publish their crypto-asset white paper, and, where applicable, their marketing communications, on their website, which shall be publicly accessible, by no later than the starting date of the offer to the public of those crypto-assets or the admission of those crypto-assets to trading on a trading platform for crypto-assets. The crypto-asset white paper, and, where applicable, the marketing communications, shall remain available on the issuer's website for as long as the crypto-assets are held by the public*»[235].

- **Article 11:** the modifications to the white papers and marketing communications are highly regulated as well thanks to the fact that the MiCA regulation is setting proper timing, breaking down and procedures. The risk of an item being heavily changed after its publishing has to be mitigated as, in fact, it is quite relevant, considering the technology behind the crypto-assets.

- **Article 13:** this one provides the behavior guidelines for the issuers, even in relation to the customers. In particular, point 2 states that «*Issuers of crypto-assets, other than asset-referenced tokens or e-money tokens, shall act in the best interests of the holders of such crypto-assets and shall treat them equally, unless any preferential treatment is disclosed in the crypto-asset white paper, and, where applicable, the marketing communications*»[236].

- **Article 14:** this is another important Article as it sets the liabilities responsibility of the issuers for misleading information disclosed in the white paper.

Point 1 defines clearly the responsibility of the issuers: «*Where an issuer of crypto-assets, other than asset-referenced tokens or e-money tokens, or its management body has infringed Article 5, by providing in its crypto-asset white paper or in a modified crypto-asset white paper information which is not complete, fair or clear or by providing*

[235] Art 8 (1), MiCAr.
[236] Art 13 (2), MiCAr.

information which is misleading, a holder of crypto-assets may claim damages from that issuer of crypto-assets, other than asset-referenced tokens or e-money tokens, or its management body for damage caused to her or him due to that infringement.

Any exclusion of civil liability shall be deprived of any legal effect» [237] but point 2 states that it is responsibility of the holder of the crypto-asset to present evidence: «*It shall be the responsibility of the holders of crypto-assets to present evidence indicating that the issuer of crypto-assets, other than asset-referenced tokens or e-money tokens, has infringed Article 5 and that such an infringement had an impact on his or her decision to buy, sell or exchange the said crypto-assets*»[238].

b) <u>For the CASP category</u>:

- **Article 59**: Just like the Article 13 for the issuers, this Article sets the general behavior provisions for the management of the crypto-assets service providers. This Article is probably even more important than the Article 13, as the management of the CASP (which can be, for example, a crypto-exchange with millions of active users) has a much higher (and more direct as well) impact on the customers.

- **Article 64**: This curious but useful Article sets provisions in defining the procedures to be performed by the CASP in order to correctly handle the customer complaints. As it does not address any direct risks arising for the customers, it is undeniably a clear example of the effort put in place by the Commission is protecting the final customers.

In addition, other than the specific articles described above for the issuers and the CASPs, the Title VI, which is dedicated to the prevention of market abuse, sets complementary provisions:

- **Article 77**: this Article manages the information disclosed by the issuers, setting a clear policy of complete, correct and updated information released to the public. «*Issuers of crypto-assets shall inform the public as soon as possible of inside*

[237] Art 14 (1), MiCAr.
[238] Art 14 (2), MiCAr.

information which concerns them, in a manner that enables the public to access that information in an easy manner and to assess that information in a complete, correct and timely manner»[239].

- **Article 80**: It is probably one of the most important articles in the entire MiCAr, not only from the customers protection perspective, but also in general.

The article, in fact, is structured on 2 points: the first one explaining the various activities prohibited and the second one giving some explicit examples, eliminating any possible grey gap and creating directly-applicable cases. Due to the high importance of the articles, and to the length as well, it must be entirely reported below:

«*No person shall engage into market manipulation which shall include any of the following activities:*

(a) unless the person entering into a transaction, placing an order to trade or engaging in any other behaviour establishes that such transaction, order or behaviour has been carried out for legitimate reasons, entering into a transaction, placing an order to trade or any other behaviour which:

i) gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a crypto-asset;

ii) sets, or is likely to set, the price of one or several crypto-assets at an abnormal or artificial level.

(b) entering into a transaction, placing an order to trade or any other activity or behaviour which affects or is likely to affect the price of one or several crypto-assets, while employing a fictitious device or any other form of deception or contrivance;

(c) disseminating information through the media, including the internet, or by any other means, which gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of a crypto-asset, or is likely to secure, the price of one or several crypto-assets, at an abnormal or artificial level, including the dissemination of rumours, where the person who made the dissemination knew, or ought to have known, that the information was false or misleading.

2. The following behaviour shall, inter alia, be considered as market manipulation:

[239] Art 14 (2), MiCAr.

(a) securing a dominant position over the supply of or demand for a crypto-asset, which has, or is likely to have, the effect of fixing, directly or indirectly, purchase or sale prices or creates, or is likely to create, other unfair trading conditions;

(b) the placing of orders to a trading platform for crypto-assets, including any cancellation or modification thereof, by any available means of trading, and which has one of the effects referred to in paragraph 1(a), by:

i) disrupting or delaying the functioning of the trading platform for crypto-assets or engaging into any activities that are likely to have that effect;

ii) making it more difficult for other persons to identify genuine orders on the trading platform for crypto-assets or engaging into any activities that are likely to have that effect, including by entering orders which result in the destabilisation of the normal functioning of the trading platform for crypto-assets;

iii) creating a false or misleading signal about the supply of, or demand for, or price of, a crypto-asset, in particular by entering orders to initiate or exacerbate a trend, or engaging into any activities that are likely to have that effect;

(c) taking advantage of occasional or regular access to the traditional or electronic media by voicing an opinion about a crypto-asset, while having previously taken positions on that crypto-asset, and profiting subsequently from the EN 102 EN impact of the opinions voiced on the price of that crypto-asset, without having simultaneously disclosed».

It must be noted that, in the MiCA regulation, other than in the Articles now descripted above, there are many other Articles in which the regulatory approach towards the customer-protection can be noticed.

CHAPTER III

AS-IS TO-BE ANALYSIS OF THE CRYPTO-ASSETS LANDSCAPE

1. Where the EU is

As it has been described in the first chapter, the current EU regulatory framework for crypto-assets is definitely not homogeneous, and most importantly, not comprehensive of the various items circulating nowadays in the market, since the regulatory approach remains security-oriented (i.e. regulation depends on the nature of the crypto-asset, rather than on the CASP/issuer/customer characteristics), and not entities-oriented.

Currently, the crypto-assets regulatory landscape remains pretty much unregulated, with the exception of the MiFID II, regulation totally not suitable for regulating crypto-assets: as already described in the previous chapters, only if a crypto-asset qualifies as a financial instrument, its usage is fully regulated by such regulation. Theoretically, it would be straightforward to think that this phenomenon would largely help in crypto-asset regulation: this is not true, as one of the main features of crypto-assets is their heterogeneous nature, which multiple types of items falling under the same, general, definition.

Apart for the MiFID II, which is the main existing tool which partially helps to regulate crypto-asset, waiting for an ad-hoc crypto-asset regulation (such as the MiCAr), the other existing legislations are the AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism), which indirectly helps to regulate certain aspects of the market entities (especially CASP and end-customers), and the EMD2 (Seconds Electronic Money Directive), which regulates the electronic money entities, and therefore its regulatory mechanism for crypto-assets is the same of the MiFID II one (the EMD2 if fact only helps if the crypto-asset falls in the electronic money category).

Apart for these three tools (MiFID II, AML/CFT, EMD2), which they have primary regulation objectives completely different from the crypto regulation, the EU

regulatory gap for crypto-asset is enormous, and the MiCA regulation is necessary to at least regulate a large portion of it.

In addition to the complete lack of regulation for the existing gap, another important risk is present in the narrow portion of currently regulated crypto-assets: EU regulatory fragmentation. In fact, the regulatory fragmentation in the European Union, caused by the different national laws applied by the different NCAs, pose the unmitigated risk of circumvention of an existing (and apparently bullet-proof) legal framework.

The mechanism is the same for banking rights approvals, in which the entire EU banking network is controlled by the ECB, delegating to NCAs the regulation of the less-impactful entities: as it is not feasible to replicate the same approach for crypto-assets regulation (especially CASP access grating, as seen in the chapter two), the MiCA regulation has to define not only the different aspects of the regulation, but also the regulating approach (as well as the "strictness") which has to be applied by the different NCAs, limiting cases of NCAs granting dubious accesses or not strictly applying the existing rules, resulting in the creation of *crypto-heavens*.

The direction the EU wants to pursue is clear and straightforward: regulating the gap in the current legislation, avoiding any disaster scenario in which it would be too late to operate. Last years of crypto-market expansion and usages however pose a serious risk of EU being too late to intervene and, most importantly, to correct any regulation misalignment with market needs: in a recent interview in fact, ECB President Christine Lagarde said that «I have said all along the crypto assets are highly speculative, very risky assets. […] My very humble assessment is that it is worth nothing. It is based on nothing, there is no underlying assets to act as an anchor of safety»[240] .

What must be defined, other than the regulatory framework (regulation principles and regulation approach), it's the approach to the technology itself. While it is true that, in this particular case, President Lagarde is giving her personal opinion in an interview, it is also true that the direction the ECB chooses is highly influenced by its president. In addition, even if the MiCA regulation (but more in general, the cryto-assets regulation) is

[240] Interview of May, the 22nd for the Dutch tv Programme "College Tour", electronically available at: https://www.npo3.nl/college-tour/22-05-2022/KN_1729332.

promoted by the EU Commission, the ECB opinion could highly impact and influence the regulatory approach adopted by the EU. In the same interview mentioned above, President Lagarde comments on uprising crypto-assets such as innovative cryptocurrencies and NFT revealed that ECB intention would be to boost the implementation of digital fiat currencies rather than improving the spread and usage of existing crypto-assets.

The implicit intention of steering the customers away from the decentralized crypto-assets (a noting that crypto-assets are not only digital currencies, thinking for example to the NFT) has obvious intention to protect and preserve the customers and the EU financial stability: suppressing an uprising sector however, with severe regulation, it is not the road the EU wants to pursue.
Currently, the MiCA regulation draft has a completely different underlying intention, which seems, at least initially, more "*technology-development"* oriented.

2.Where the EU wants to be

As said in the paragraph above, what it's missed in today's regulation (apart for the proper regulation of large portion of assets, in the specific case of crypto-assets) is an harmonized approach to the matter. Such problem, in the specific case of crypto-assets must be addressed, considered the boundaries-free nature of the technology itself.

What the current draft of MiCAr brings is a harmonized approach, defining one general regulation framework, to all crypto-assets currently not covered by the EU legislation: the MiCA regulation in fact will cooperate with existing laws (MiFID II, EMD2, etc.), and not taking over their regulation on crypto-assets. The guideline in understanding which regulatory framework must be applied is really straightforward, as we will see in a scheme below: "Does such asset fall in the categories already regulated?".

The initial assessment on the nature of the asset examined is simplified by the presence of clear but comprehensive definitions both in MiCAr and in the MiFID II, as seen in the previous chapters.

Regarding the assets regulated by the MiCAr, one key feature which will greatly simplify and harmonize the NCAs approach is the presence of a *all-inclusive* category, used as a container for all those crypto-assets non falling into the financial instrument (MiFID II), e-money (EMD2), ART and EMT categories. In fact, as we will see, the MiCA regulation is the last piece of law preventing the unregulation gap, and the *catch-everything* category is necessary.

In particular, the Title II of MiCAr is design to «regulate the offerings and marketing to the public of crypto-assets other than asset-referenced tokens and e-money tokens»[241]. Obviously, the requirements, as well as the principles, are very generic, but this at least puts some initial regulations on a broad category which would completely escape the EU legislation. Further improvements, also based on specific sub-categories of assets which will be created, can always be made.

Returning to ARTs (asset referenced tokens), such category is explicitly regulated in an ad-hoc Title (number III), as the main points are:

- Chapter 1 «describes the procedure for authorisation of asset-referenced token issuers and the approval of their crypto-asset white paper by national competent authorities»[242];

- Chapter 2 «sets out the obligations for issuers of asset-referenced tokens»[243];

- Chapter 4 «sets out the rules for the acquisition of issuers of asset-referenced tokens»[244];

- Chapter 5 «sets out the criteria that EBA shall use when determining whether an asset-referenced token is significant»[245];

- Chapter 6 «obliges the issuer to have a procedure in place for an orderly wind-down of their activities»[246].

[241] On this particular matter, see MiCA regulation at page 10.
[242] On this particular matter, see MiCA regulation at page 11.
[243] *Ibid.*
[244] *Ibid.*
[245] *Ibid.*
[246] On this particular matter, see MiCA regulation at page 12.

Similarly, for the EMTs (e-money tokens) there's an ad-hoc Title as well (IV). The main points are:

- Chapter 1 «describes the procedure for authorisation as an issuer of e-money tokens»[247];

- Chapter 2 sets out the requirements for e-money classification[248];

As before anticipated, the first question to be responded in examining a new *crypto-like* asset will be whether it could be classified not only as a crypto-asset (using the definition «'crypto-asset' means a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology»[249]) but also, and firstly, as a financial instrument (using the financial instrument list defined in the MiFID II) or as an electronic money (as defined in the EMD2).

The answer to such, apparently, easy question can only be given after an extensive analysis of the item, consisting in assessing its specific features, rights granted, functioning, underlying specific risks, etc.
If, and only if, the analysis gives a negative result for both MiFID II and EMD2, the MiCA regulation can be taken into consideration.

As already mentioned in the paragraphs above, if the asset qualifies as a crypto-asset, it must be defined in which of the three different categories it falls into.

As noted earlier, the Title III will regulate all the crypto-asset falling – in addition to the general crypto-asset definition – even into the ART definition, hence «'asset-referenced token' means 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»[250].

[247] *Ibid.*
[248] *Ibid.*
[249] On this particular matter, see MiCA regulation at page 34.
[250] *Ibid.*

Similarly, if the crypto-asset examined misses the first category, the EMT compatibility is considered, using the following definition: «'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»[251]. As anticipated, the Title IV aims to regulate be the item examined.

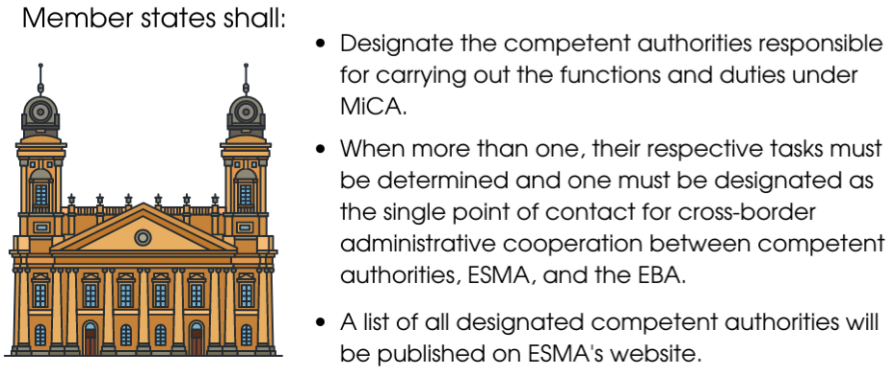
In case of another missed categorization, all the MiCAr regulatory strength will be evident: no definitions to be aligned with, nor technical requirements to be satisfied. The single requirement in order to fall in the third category is, apart for the general crypto-asset definition obviously, not falling into the ART and EMT categories.

It will be a powerful tool, leaving out any problems in considering whether the item should be regulated or not.

Under this broad and – for regulatory needs – heterogeneous category, one additional differentiation will be made in the legal qualification of the asset, respecting the categories reported in the first chapter (for example, if the crypto-asset has to be qualified as utility tokens, meaning that it's usage is intended to provide a digital access to a good and/or service via DLT, and cannot be traded/used as a store-of-value because it is only accepted by its issuer): this feature will not affect the take-all characteristic of the category, as it will only help to have the most appropriate laws as possible, given the high degree of the variability in this group.

[251] *Ibid.*

The practical implications of this differentiation will be only minor differences in the Title II, with a special attention given to utility tokens and the risks of their unappropriated usage.



MiCA explained: the EU crypto-asset law. The proposed Markets in Crypto-asset Regulation - XReg Consulting LTD

In relation to the entities involved in the supervision, the central role will be performed by the various NCAs, with a general supervision of the ECB, ESMA and EBA, as specified in various articles. One article in particular defines also the cooperation of the various NCAs between themselves, as well as with the supervisory entities (ECB, ESMA and EBA).

The related Article is Article 83(1), which states: «*Competent authorities shall cooperate with each other for the purposes of this Regulation. They shall exchange information without undue delay and cooperate in investigation, supervision and enforcement activities. Where Member States have chosen, in accordance with Article 92(1), to lay down criminal penalties for an infringement of this Regulation, they shall ensure that appropriate measures are in place so that competent authorities have all the necessary powers to liaise with judicial, prosecuting, or criminal justice authorities within their jurisdiction to receive specific information related to criminal investigations or proceedings commenced for infringements of this Regulation and to provide the same information to other competent authorities as well as to the EBA and ESMA, in order to fulfil their obligation to cooperate for the purposes of this Regulation*»[252].

[252] Article 83 (1), MiCAr.

2.1. Possible unregulated crypto-assets?

As a matter of fact, the regulatory framework is well established, and if not heavily changed in the definitive version, all the categories of crypto-assets seem to be regulated, with the related risks properly addressed, thanks also to the catch-all category trick.

The straightforward and main question that the Commission (but also the public) tried to answer once prepared the draft of the MiCA regulation is: "would there be any crypto-asset or crypto-like asset still not regulated?".

The answer seems easy, but the reality is much more complex. The answer, is in fact no: there will not be any crypto-asset unregulated, but there still will be many crypto-like asset unregulated. Even though the answer may seem contradictory, there are a lot of crypto-like assets, also based on DLT technology, which may not enter in the MiCAr definition, as the main criteria is exactly this: "how much appropriate is the definition of crypto-asset for the asset under analysis?". The main concept here is that, **while it is true that MiCA regulation will impact every crypto-asset, it is also true that not every crypto-like asset will be "labeled" as crypto-assets.**

The best example for such category of items is the NFT.

The NFTs (abbreviation of *Non-fungible tokens*) are a typology of digital asset, representing real objects like videos, music, art, but they can also be applied to real-life events as well (such as the 1969 moon landing, which can be acquired on the digital NFT marketplace "OpenSea"[253]). Such particular category of items gain extreme popularity after the initial draft of MiCAr, therefore the regulation left this particular items partially out of scope. The NFT market skyrocketed hugely in 2021: the trading of NFTs in the new-born marketplaces in 2021 increased by more than 17 billion of dollars, up by a percentage of over 21,000% in relation to 2020's total worth of 82 million of dollars[254].

Considering the uprising numbers of such market, it would pose a serious risk to completely disregard such phenomenon as the only regulation of NFTs in fact will consist in the same mechanism saw for the MiFID II: only the NFTs falling in the crypto-asset

[253] On this particular matter see the following example at this link: https://opensea.io/assets/ethereum/0x495f947276749ce646f68ac8c248420045cb7b5e/110544443712593882381876477537605751177351678404406052250850952914623612846081.

[254] On this particular matter, see the following article: https://www.pymnts.com/nfts/2022/nfts-hit-17b-in-trading-in-2021-up-21000/.

category (in accordance with the definition) will be subjected to MiCAr regulatory obligations.

Within the 2023 the European Commission planned to completely address the risks related to NFTs with an initial assessment and definition of a proper, horizontal legislation, defining an appropriate framework which will be integrated with MiFID II, EMD2 and MiCA regulation[255].

In relation to crypto-assets falling into the category "different from ART and EMT", offered to the public and/or traded on trading platforms before the effective application of MiCAr, there will be the issue of lack of retro-activity, meaning that the issuers of such category of crypto-assets will be exempted by the provisions of Title II, in particular to the obligations requiring to be a legal entity, the white-paper preparation and the – also ethical – rules of conduct.

Help on this point will be given by the Market Abuse Regulation, covering the time gap until MiCAr effective implementation, in particular with the Article 18, which will partially cover and mitigate the risks underlying the issue of crypto-assets different from ART or EMT.

Moreover, since the MiCAr implementation date such category of crypto-assets will be immediately required to comply to Title V (CASP) and Title VI (prevention of market-abuse): therefore, the underlying risks should be considered well mitigated.

Another major concern would be the "issuerless crypto-asset" typology. Issuerless crypto-asset typology are all the crypto-assets of which the issuer cannot be identified: the most famous example is "Bitcoin". In such decentralized finance projects in fact, once the code is released, the platform uses smart contracts to perform the actions needed. As the actions are performed automatically via code execution, in accordance with the rules programmed, no active management is further needed[256]. As already seen in the first

[255] On this particular matter, see the following article: https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/.

[256] On this particular matter, see COELHO-PRABHU S., (2020), *A Beginner's Guide to Decentralized Finance (DeFi)*, electronically available at *The Coinbase blog*: https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4?gi=2e472571042d.

chapter, this lack of a central entity responsible for the platform functioning pose a serious risk in relation to who should be targeted on a regulatory level.

In order to address the risks, the MiCAr approach is very simple:

1) Firstly, as previously said, there will not be any problems of non-applicability due to the "crypto-asset" definition being sufficiently wide to catch all the different items in the market. In addition to this, it is worth noting that the regulatory framework labels as "issuer" not necessarily the person involved in the creation of the asset.

   The "Issuer" definition present in the MiCA regulation is in fact broad enough, with the same catch-all approach used for the crypto-asset definition: «'issuer of crypto-assets' means a 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-assets»[257]. Issuers are, in fact, all the people involved not only in the creation of the asset itself, but also on its entrance into the market.

   As a matter of fact, during July 2022, on this particular aspect, the Belgian Financial Services and Markets Authority prepared a chart in order to clarify any doubts: once the MiCAr will take effect, even the trading platforms will be required to issue a "White paper" like document[258].

   Nowadays at least some "facilitators", requesting the crypto-assets access to the trading platforms, can always be indicated: therefore, the underlying risks seems to be well mitigated.

2) Secondly, an interesting point is the necessity to be a legal person to be an issuer, as stated in the definition reported above: this does not mean that every issuer who is not a legal person (but for example, only being a natural person) would be out of MiCAr scope. It is, in fact, exactly the opposite: if a natural person is labeled as an "issuer" (for example by looking for the crypto-asset admission on the major trading platforms, or by trying to sell its technology to third parties, or simply

[257] Art 3 (6), MiCAr.
[258] On this particular matter, see ANDERSEN, (2022), *Belgian regulator reviews crypto asset classifications while awaiting harmonization*, electronically available at *CoinTelegraph*: https://cointelegraph.com/news/belgian-regulator-reviews-crypto-asset-classifications-while-awaiting-harmonization.

because it created it) would contrast with the MiCA regulation, and therefore it would be targeted by the NCA and its supervisory powers.

The supervisory powers can vary, depending on the magnitude of the infraction: from an administrative sanction to complete prohibition in order to continue with the crypto-asset issuance, de-facto completely blocking its entrance into the market.

Posing this requisite, the risk of inadequate issuance (as well as inadequate entity issuing the asset) is completely addressed.

Having analyzed the impact that the Market in Crypto-Asset Regulation will have, especially assessing the magnitude of the possible problems, the real question is: is the MiCA regulation the definitive regulation for all the crypto-assets different aspects?

The answer is: while it is true that all types of crypto-assets are regulated, along with proper mitigation of the risks arising in the grey areas (such as the special occurrences analyzed in this chapter), as (at least initially) there are no leftovers thanks to the fact that MiCA regulation is, definitely, customer protection oriented. It would help to have an harmonized framework for specific areas also, such as the customer taxation criteria, eliminating any possible misalignment between member states.

Another point is the technological advancement: technology runs fast, much faster than the regulation process: if the European Union wants to always have a fully regulated crypto-asset landscape, the Commission will be definitely being required to often update the regulation, including any possible technology-specific provision.
Definitely, MiCAr is the proper base to build on the future expansions of the regulation of this matter.

2.2. MiCAr agreement

On June the 30th 2022, the Council presidency and the European Parliament reached a provisional agreement on the MiCAr proposal text, without any relevant change to the Articles[259].

[259] EU Council press release of June, the 30th, electronically available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

Mondaq, October the 19th 2022, LEE J., KRAMPETSOS M, A Game Changer For Blockchain Regulation: The EU's Crypto Rules Reach The Final Stage, electronically available at:

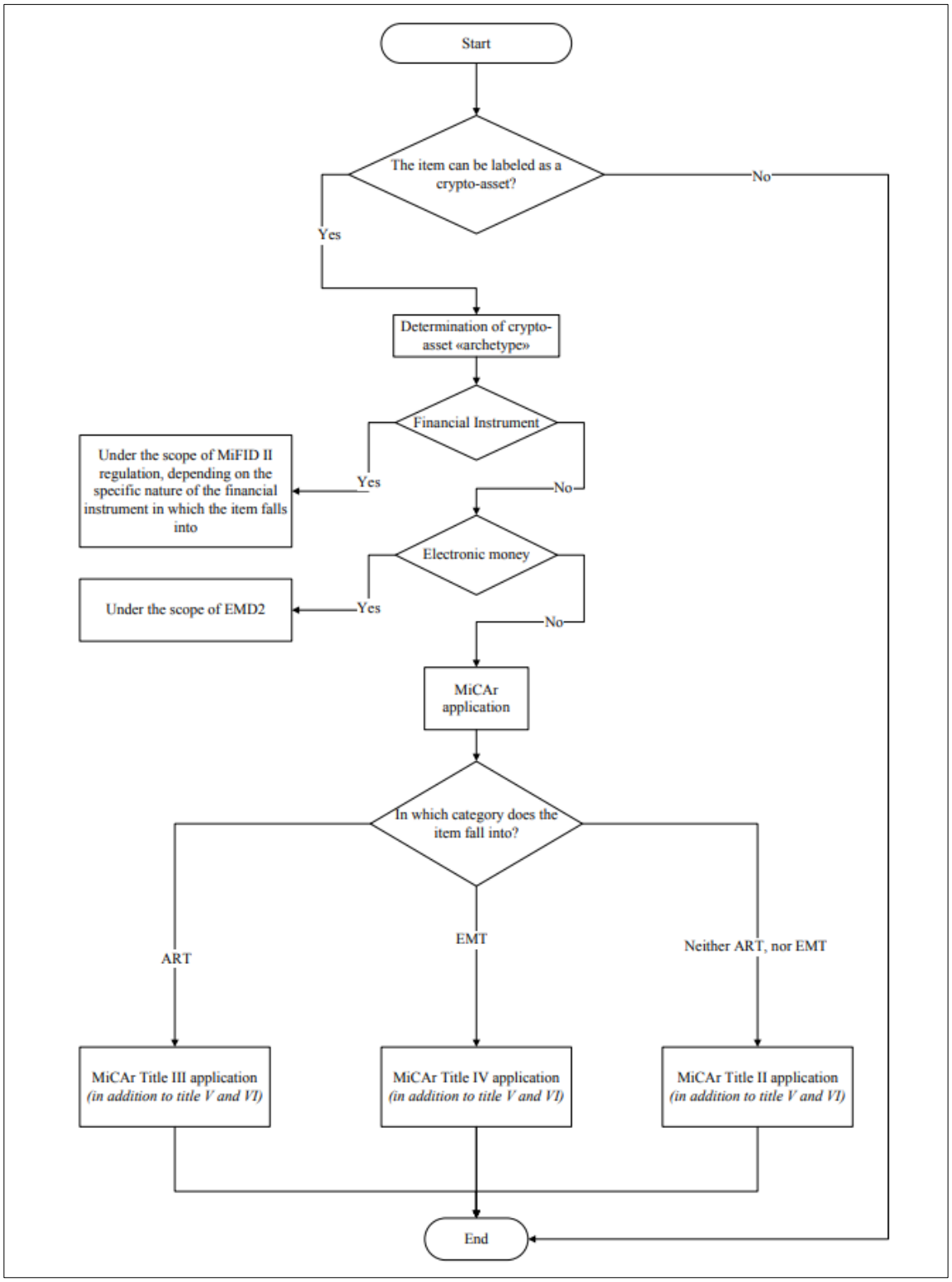
https://www.mondaq.com/uk/fin-tech/1241818/a-game-changer-for-blockchain-regulation-the-eu39s-crypto-rules-reach-the-final-stage

The small changes made are regarding the reinforcement of the safety measures, such as the allocations of specific reserves and the implementation of redemption plans for crypto-assets whose value is in distress[260]. This supplementing measures reflect the attention given by the EU to the current situation of the most popular (and impactful) crypto-asset category, the crypto-currencies, as it is easy to note that such increased measures address the direct risks arising from the excessive value fluctuations.

Worth noting is that this is only the first step of the adoption of the MiCAr regulation, as it is only a provisional agreement, as the formal adoption procedure has to continue.

[260] On this particular matter, see BERGER S., (2022), *Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets*, electronically available at *Legislative Train Schedule*: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-crypto-assets-1 .

Logical process flow after the MiCAr framework implementation



CONCLUSIONS

This thesis aimed to provide an overview to the regulatory future of crypto-assets in the Union by an analysis of the newly proposed Regulation on Markets in Crypto-assets in its published version of the 24th of September 2020. The present work has presented the current stage of the debate on how the regulatory future of crypto-assets in the European Union could present itself as the Commission's proposal (MiCAr) is not a legislative act in force.

As explained so far, the MiCA regulation lays down a harmonized framework for crypto-assets currently not falling within the scope of existing European financial services legislation. The proposal tries to transpose the currently unregulated market of crypto-assets in a highly regulated market along the lines of the already existing European financial services legislation.

Intelligently, the Commission adopted a comprehensive approach, finding the correct balance between the market safety and the excessive bureaucracy: this regulation should in fact support the innovation of the crypto-sector as well as ensuring the fair competition while assuring the market integrity, both for the issuers, the CASP and the final customers.

Moreover, such regulation is well integrated with existing ones, specifically addressing the grey gaps left out (for example, by the MiFID II and the EMD2), without risky overlapping of contradictory provisions.

Although not fully completed, and more importantly, with a limited life expectancy, as – due to the specific technology of this sector – it will be frequently requested to be updated, the MiCA regulation successfully addresses the risks of the crypto-assets usage, and sufficiently fills the existing legislative grey gaps.

BIBLIOGRAPHY

ANDERSEN D., (2022), *Belgian regulator reviews crypto asset classifications while awaiting harmonization*, electronically available at *CoinTelegraph*: https://cointelegraph.com/news/belgian-regulator-reviews-crypto-asset-classifications-while-awaiting-harmonization

AURUS, *Aurus token white paper*, electronically available at: https://aurus.io/aurus-whitepaper.pdf

BULLMAN D., CARDONE L., DELCROIX A., FORNARO D., KAUFMANN C., KIEWIT G., KOCHANSKA U., KONDRAKA E., KÖRNER J., LÖBER K., MAYERS M., PINNA A., PALLIGKINIS S., TRACZ A. and VOULDIS A., (2019), *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, ECB Occasional Paper Series No.223/Maggio 2019, electronically available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

CATALINI C. and GANS S.J., (2018), *Initial Coin Offerings and the Value of Crypto Tokens*, MIT Sloan Research Paper No. 5347-18, electronically available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137213

COELHO-PRABHU S., (2020), *A Beginner's Guide to Decentralized Finance (DeFi)*, electronically available at *The Coinbase blog*:
https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4?gi=2e472571042d

COUNCIL OF THE EUROPEAN UNION, (2019), *Joint Statement by the Council and the Commission on Stablecoins*, electronically available at: https://www.consilium.europa.eu/it/press/press-releases/2019/12/05/joint-statement-by-the-council-and-the-commission-on-stablecoins/

CNMV and BANCO DE ESPAÑA, (2018), *Joint press statement on 'cryptocurrencies' and initial coin offerings*, electronically available at:

https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/presbe2018_07en.pdf

DOWLAT S. and HODAPP M., (2018), *ICO Quality: Development & Trading*

EBA, (2019), *Report with advice for the European Commission on crypto-assets*, electronically available at: https://eba.europa.eu/eba-reports-on-cryptoassets

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

ESMA, SECURITIES AND MARKETS STAKEHOLDER GROUP, (2018), *Own initiative Report on initial coin offerings and crypto-assets*, electronically available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf

ESMA, (January 2019), *Advice on Initial Coin Offerings and Crypto-Assets*, electronically available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

ESMA, (2019), *Report on Licensing of FinTech Business models*, electronically available at: https://www.esma.europa.eu/sites/default/files/library/esma50-164-2430_licensing_of_fintech.pdf

ESMA, (2019), *Annex I – legal qualification of crypto-assets – survey to NCAs*, electronically available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1384_annex.pdf

EUROPEAN COMMISSION, (2020), *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets and amending Directive (EU) 2019/1937*

(MiCA), electronically available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

FATF (2019), *Guidance for a risk-based approach: virtual assets and virtual asset service providers*, electronically available at: "https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

FD2A, AMAFI, AFG and ASPIM, (2019), *The FD2A, AMAFI, AFG and ASPIM measure the interest of actors for "security tokens". Questionnaire on security tokens – summary of results*, electronically available at: http://www.amafi.fr/download/pages/2qnY1c7mzJspXmuzqEZWD6blcihezxug2Vgpt32a.pdf

FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION, EUROPEAN COMMISSION, (2020), *Communication on Digital Finance Package*, electronically available at: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

FINANCIAL STABILITY BOARD, (2019), *Regulatory issues of stablecoins*, electronically available at: https://www.fsb.org/wp-content/uploads/P181019.pdf

FMA, (2018), *Bitcoin & Co*, electronically available at: https://www.fma.gv.at/en/fintech-point-of-contact-sandbox/fintech-navigator/bitcoin-co/

G7 WORKING GROUP ON STABLECOINS, (2019), *Investigating the impact of global stablecoins*, electronically available at: https://www.bis.org/cpmi/publ/d187.pdf

HACKER P. and THOMALE C., (2017), "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law", *European Company and Financial Law Review 645-696*, p 20 ff., electronically available at: https://ssrn.com/abstract=3075820 or http://dx.doi.org/10.2139/ssrn.3075820

HOUBEN R. and SNYDER A., (2020), *Crypto-assets: Key developments, regulatory concerns and responses*, Study PE 648.779, electronically available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf

HM TREASURY CRYPTOASSETS TASKFORCE (October 2018), *Financial Conduct authority and Bank of England*: *final report*, electronically available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf

IOSCO, (2020), *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*, electronically available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf

LAWYER L., (2022), *Asset-Referenced Tokens Under the EU's Proposed Markets in Crypto Assets Regulation*, electronically available at *Medium*: https://medium.com/coinmonks/asset-referenced-tokens-under-the-eus-proposed-markets-in-crypto-assets-regulation-458c317577bb#:~:text=Under%20MiCA%2C%20a%20crypto%2Dasset,a%20combination%20of%20such%20assets%E2%80%9D

LAURENT P., *The tokenization of assets is disrupting the financial industry. Are you ready?*, Inside magazine issue 19 – Part 02: from a core transformation/technology perspective, Deloitte, 2018, p. 6 ff.

MASS T., (2019), *Initial coin offerings: when are tokens securities in the EU and US?*, pp. 21-23, electronically available at: https://ssrn.com/abstract=3337514

OECD, (2020), *The Tokenisation of Assets and Potential Implications for Financial Markets*, electronically available at: https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm

OMFIF and IBM, (2019), *Retail CBDCs. The next payments frontier*, electronically available at: https://www.omfif.org/wpcontent/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf

RAO M.R. and VATRAPU R., (2021), *Distributed ledger technologies and blockchain for FinTech: Principles and applications, The Routledge Handbook of FinTech*, Routledge, p. 79 ff.

RAUCHS M., GLIDDEN A., GORDON B., PIETERS C.G., RECANATINI M., ROSTAND F., VAGNEUR K. and ZHENG Z.B., (August 2018), *Distributed Ledger Technology Systems: A Conceptual Framework*, electronically available at: https://ssrn.com/abstract=3230013 or http://dx.doi.org/10.2139/ssrn.3230013

RAUCHS M., BLANDIN A., KLEIN K., PIETERS G., RECANATINI M., ZHANG B., (December 2018), *2nd Global crypto-asset benchmarking study*, Cambridge Centre for Alternative Finance, electronically available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf

SNYERS A. and PAUWELS K., (2019), *De ITO: a new kid on the block in het kapitaalmarktenrecht*, Larcier, Bruxelles, p. 122 ff., electronically available at: https://hdl.handle.net/10067/1621030151162165141

XREG CONSULTING LTD, (2020), *MiCA explained: the EU crypto-asset law. The proposed Markets in Crypto-asset Regulation*, electronically available at https://uploads-ssl.webflow.com/5df7642ffbd9264804671001/5f7b3b3116ebd4add01abd32_XReg%20EU%20MiCA%20explained%20-issue%201-1.1a%20-FINAL.pdf

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

ZETSCHE D.A., ANNUNZIATA F., ARNER D.W. and ROSS R.P., (2020), *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy*, European

Banking Institute, Working Paper Series 2020/77, electronically available at: http://dx.doi.org/10.2139/ssrn.3725395