Ca' Foscari
University
of Venice

Master's Degree Programme
in Finance

Final Thesis

New Game, New Rules

The Current and Upcoming Regulatory Framework for Crypto Exchange Platforms

Supervisor
Ch. Prof. Andrea Minto

Graduand
Alessia Tortato
868960

Academic Year
2021/2022

Abstract

According to Forbes, there are nearly six hundred Crypto Exchange Platforms worldwide, populating the flourishing crypto asset market. Exchanges are now playing a crucial role for investors and consumers, who are increasingly using them to trade crypto assets.

However, Authorities pointed out the new risks arising from this market, claiming the need to keep up the pace in the creation of a sound legal framework for crypto assets and the infrastructures in which they are exchanged, in order to mitigate them. In fact, the current regime foresees the adaptation of existing rules, which however rarely fit the new paradigm, leaving the vast majority of assets and providers unregulated.

The need for a bespoke regime, in particular for Crypto Asset Service Providers, brought to the development of the Market in Crypto Assets Regulation as part of the Digital Finance Package which, together with a proposal for an Anti-Money laundering Package, represents a possible path toward the creation of a level playing field for market players, reducing potential risks for consumers while boosting the Single Market and the Capital Markets Union.

Keywords: Crypto Asset Service Providers, Exchanges, MiCAR, MiFID, Anti-Money Laundering

Table of Contents

Introduction

According to Forbes,[1] there are nearly six hundred Crypto Exchange Platforms worldwide, populating the flourishing crypto asset market. Exchanges are now playing a crucial role for investors and consumers, who are increasingly using them to trade crypto assets.

It is widely agreed that Blockchain and DLTs in general have the potential to spur financial innovation, and to provide new solutions to a fast-changing world. This is shared by the European Union Regulator, which in fact started the text of the Communication on a Digital Finance Strategy with the following words:

"The future of finance is digital: consumers and businesses are more and more accessing financial services digitally, innovative market participants are deploying new technologies, and existing business models are changing".[2]

In fact, the project revolves around the digital transition of the European Union, which would cover the leading role in Digital Finance areas, making it an example to follow by others.

This would bring notable benefits both to consumers and businesses, providing, for example, alternative financing to consumers and small and medium enterprises for which traditional financing would be difficult, but also enhancing financial inclusion.

However, Authorities pointed out the new risks arising from this market, claiming the need to keep up the pace in the creation of a sound legal framework for crypto assets and the infrastructures in which they are exchanged, in order to mitigate them.

The current regime foresees an adaptation of existing rules, which however rarely fits the new paradigm, leaving the vast majority of assets and providers unregulated.

[1] Javier Paz, "The Best Global Crypto Exchanges" (Forbes, March 2022)
[2] European Commission "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU", COM (2020) 591 final.

This harms investors and produces a negative effect provided the cross-border nature of crypto assets and exchanges, increasing fragmentation at the European level and creating regulatory arbitrage. Those downsides are eventually enhanced as single jurisdictions opted for the creation of their own rules, on the one hand safeguarding their own citizens but on the other, contributing to the creation of an uneven playing field.

Hence, the need for a bespoke regime, in particular for Crypto Asset Service Providers, brought to the development of the Market in Crypto Assets Regulation as part of the Digital Finance Package which, together with a proposal for a more stringent Anti-Money laundering legislation, represents a possible path towards the creation of a sound system for market players, which would not have to adapt to new rules and would have reduced costs of compliance.

The upcoming regulatory framework would in fact contribute to the reduction of potential risks for consumers while boosting the Single Market and the Capital Markets Union.

The dissertation is developed as follows.

The First Chapter provides some preliminary remarks on the characteristics of Exchange Platforms for crypto assets, explaining the main differences between Centralized Exchanges and Decentralized ones.

The Second Chapter instead proposes an overview of the main benefits and risks posed by providers of services in relation of crypto assets, laying the basis for the subsequent chapters, namely stating the reasons for which the Authorities are seeking to regulate the sector.

The Third Chapter provides instead a description and analysis of the current regulatory framework for Providers, explaining in which ways the relevant existing rules may be applied to the innovative instruments and their providers, also through some examples of National Initiatives.

The Fourth and final Chapter instead proposes an overview of the Upcoming Regulatory Framework at the European Union, whose aim is to make clear the regulatory perimeter

and introduce specific rules for Crypto-Assets Service Providers, bringing higher legal certainty.

Finally, three short analyses on themes of *Blockchain Forensics*, *DeFi Regulatory Challenges* and a *New possible definition of Financial Instrument* will be provided in the Annexes.

Chapter I: Preliminary Remarks on Exchanges

Crypto exchange platforms are trading systems whose ultimate goal is to enable users to buy and sell crypto assets, matching their demand and supply after the initial placement, allowing for the trade in exchange of fiat currency, other crypto assets, or both.

Exchange platforms rely on Distributed Ledger Technology[3] and, in particular, on blockchain, which was first introduced in finance by Satoshi Nakamoto in his Whitepaper on bitcoin,[4] whose primary aim was to promote the exchange of cryptocurrencies in a decentralized manner, taking off the centralized trusted party role which was deemed to be responsible for the earlier Great Financial Crisis.[5]

Distributed Ledger Technology is used in order to enable the creation of a network of users, namely the nodes, whose role is that of running a decentralized peer-to-peer network for the approval, verification, and exchange of data. Each transaction taking place on the blockchain is validated by the nodes, and related data are then collected in blocks which, once filled, are closed and linked to the previous ones with a crypto key or algorithm, thus forming a chain from which the name blockchain is derived. In fact, blockchain technology is used in combination with cryptography,[6] granting on the one hand that transaction information is fully protected and not repudiable and, on the

[3] Blockchain represents one form of DLT; as explained in the Cryptonomist article "The Differences between Blockchain and Distributed Ledger Technology (DLT)", "Blockchain and DLT are both distributed decentralized ledgers that proceed by applying the consensus between the nodes in a transparent and not hackable way. But blockchain is that special type of DLT that uses the chain of blocks to organize and record data and which can only be added". Blocks and the information inside them are marked with a time stamp and recorded in a chronological manner. DLTs are technologies based on distributed ledgers on which information is simultaneously saved and made available in multiple locations. They make use of cryptography, thanks to which information can be registered, validated, and made available to all participants, and cannot be modified nor altered. The technology allows on the one hand to add information without the need of a central trusted party (when consensus is reached among participants), and on the other, the immutability of information added. It makes use of a cryptographic system that uses both private and public keys.

[4] Nakamoto S., A Peer-to-Peer Electronic Cash System, 2008

[5] i.e., *The Great Financial Crisis* of 2007/2008.

[6] Instead, cryptography allows the conversion of data into private code with the use of encryption algorithms, typically for transmission over a public network.

other hand, making data redundant and thus accessible by all participants.[7] Indeed, once blocks are approved and verified,[8] they are inserted in the blockchain and therefore made available to anyone, making the stored data immutable and hence, trustworthy[9].

Blockchains can be either public or private: *public*[10] blockchains are open access and allow users to freely join them, whereas *private*[11] blockchains allow only specific nodes to participate in the network.

Typically, platforms adopt three main business schemes for the trading phase: one involves the use of a trading book for the matching of orders, the second allows for the direct trading between the parties of the transaction,[12] and finally the third allows the customer to trade with the platform manager.

Additionally, crypto exchange platforms can be classified as *Centralized* or *Decentralized*.

1.1. Centralized Exchanges

Centralized Exchanges allow their users both to exchange and store their digital assets through and within the platform on a large scale. They were first created and used in 2009; among them, New Liberty Standard[13] and Mt Gox. The latter became famous

[7] The ledger allows information to be stored and immutable, thus not prone to manipulation. Information can be continuously added without a centralized trusted party upon network consensus.

[8] Nodes shall approve blocks containing transaction data by solving a computational problem; once approved, the other nodes composing the network must then verify that the problem is correctly solved. When a node solves the computational problem and approves the block, and the other nodes verify the correctness of the solution, he/she is rewarded by the network with the native coin: this mechanism is called Proof of Work and represents one of the consensus algorithms.

[9] Due to the transparency and immutability of the ledger.

[10] In order to take part in a public blockchain no authorization by a central entity is necessary; they are open access, hence allowing nodes to participate, also from different countries. The nodes participating in open blockchains provide their own support to the network through their computational resources.

[11] Private blockchains are composed of a network of nodes that are previously authorized based on their repute, accepting vetted nodes only.

[12] Peer-to-peer model.

[13] NewLibertyStandard was the first website to sell bitcoin and a catalyst that helped bitcoin grow into what it is today.

because of the hacks it faced,[14] for example, in 2011 for a total amount of 8.75 million dollars and in 2019 for 615 million dollars.

During the following years, the exchanges panorama bloomed, in particular during 2017, which was characterized by the Initial Coin Offerings[15] boom during which, for example, Binance managed to get 15 million dollars selling its *BNB tokens*, which amounted to about half of the total supply.

According to CoinMarketCap,[16] Centralized Exchanges with the highest exchange volume are Binance, Coinbase, Crypto.com, Kraken, Kucoin, and Bitfinex.

Centralized Exchanges are user-friendly and do not require advanced knowledge[17] about crypto assets and blockchain technology in general; they offer accessory services such as the custody and safekeeping of digital assets, namely they hold clients' assets on their behalf.

The trade and settlement usually take place in the books of the platforms, hence requiring users to deposit their assets with the platform prior to trading. For this reason, they present some registration requirements, thanks to which users' identity is well verified,[18] as will be described later.

Centralized Exchanges enable users to exchange fiat currencies for crypto assets through the intervention of a payment gateway[19] with fiat currency. They work as intermediaries, and thus, they charge their users a fee in exchange for their services, which comes in the form of a percentage of the amount of digital assets exchanged.

[14] MtGox is now preparing to reimburse its clients. In this regard, see The Cryptonomist article "Mt. Gox si prepara a pagare i creditori" published in July 2022.
[15] Initial Coin Offerings are defined as operations through which companies, entrepreneurs, developers, or other promoters raise capital for their projects in exchange for crypto assets created by them.
[16] See CoinMarketCap, Exchanges section.
[17] In order to be used: of course, before buying crypto assets, users should get the basic knowledge to understand the risks they are facing as declared by European Supervisory Authorities and National Competent Authorities' numerous warnings.
[18] As will be described in Chapter 3, identity verification is required for anti-money laundering purposes.
[19] Which works as a connection with the traditional world.

The matching and execution of orders and the transfer of ownership between the exchange users are typically recorded in the platform books, namely off-chain, being registered as a change in the balance of the users' wallets.[20] Instead, when users deposit or withdraw their crypto assets at the platform,[21] the transaction is recorded on the DLT, namely occurs on-chain.

Centralized exchanges are much more user-friendly than their decentralized counterparties and are dominant today.[22] Firstly, access to a centralized exchange is provided thanks to a username and a password and, where foreseen, strong customer authentication. Moreover, they present a relatively low amount of fees.

However, custody and safekeeping services imply that users are required to hand over the control of their private keys to the platform before trades take place.

This comes with two significant implications: first, centralized exchanges become a target for hacks as they represent a single point of failure where private keys are centrally stored with user information, resulting in a high concentration of data and crypto assets within the platform.[23] Second, the settlement of trades is not dependent on DLT, resulting on the one hand in improved scalability and decreased congestion risk, but on the other, in counterparty risk with the platform.

1.2. Decentralized Exchanges

Decentralized Exchanges (DEX) consist of venues whose ultimate goal is to allow the exchange of crypto assets in a peer-to-peer manner: this type of exchange takes place

[20] Transactions involving Fiat currencies and Digital assets (Fiat-to-Digital and Digital-to-Fiat) are recorded on-chain, whereas Crypto-to-Crypto transactions only occur within the platform interface, resulting in a change of balance of the accounts involved.
[21] In exchange for fiat currency.
[22] According to KPMG report "Crypto Insights #2. Decentralised Exchanges & Automated Market Makers – Innovations, Challenges & Prospects", centralized exchanges account for 95% of exchange volumes in crypto assets; for example, Binance centralized exchange processes more than $20 billion in transactions each day, compared to Uniswap decentralized exchange with less than $2 billion.
[23] Indeed, as reported by Bloomberg, several of those platforms have been hacked. An example is the Japanese platform Coincheck.

in an automated way, thanks to the use of independent and autonomous software in a wholly disintermediated manner.[24]

Compared to centralized exchanges, *Decentralized Exchanges* present features for which a certain degree of knowledge is required, thus making them less user-friendly.

First of all, they do not host a digital wallet, which users shall create first on their own. In fact, they do not allow the safekeeping of assets, but only represent an infrastructure for the connection of users.

Decentralized Exchanges appeared first in 2013 with OmiseGO and BitShares.[25] They implemented the peer-to-peer business model were which enabled the matching of demand and supply through the use of smart contracts.[26] 2019 saw the implementation of the so-called Automated Market Maker[27] orders automation, which UniSwap[28] first provided. It consists in the automation of market orders, which also reduces liquidity issues as well as volume issues.

According to CoinMarketCap, the principal DEX players are Uniswap, SushiSwap, PancakeSwap, Serum, and Trader Joe.[29]

Many Centralized Exchanged also designed their Decentralized version; Binance is an example.[30] More than 200 decentralized exchanges can be counted, but they present a significantly lower trading volume compared to centralized ones.[31]

[24] Typically, DEXs rely on liquidity pools to function. Liquidity pools consist of pools of crypto assets that are used to eliminate the issues of illiquid markets.
[25] Websites: https://www.omise.co/ and https://bitshares.org/
[26] Gartner defines *Smart Contracts* as "a type of blockchain record that contains externally written code, and controls blockchain-based digital assets. When triggered by a specified blockchain write event, a smart contract immutably executes its code and may result in another blockchain event".
[27] As explained in the BIS article "Trading in the DeFi era: automated market-maker", "AMM protocols allow traders to exchange one cryptoasset for another automatically on a blockchain. They build on the idea that traders can become liquidity-providers by making their cryptoassets available in liquidity pools".
[28] Website: https://app.uniswap.org/#/swap
[29] Available at: https://app.sushi.com/swap https://pancakeswap.finance/ https://docs.projectserum.com/ https://www.traderjoexyz.com
[30] See https://www.bnbchain.org/en.
[31] See CoinMarketCap

The main features of Decentralized Exchanges can be summarized as follows.

First, as opposed to centralized exchanges, decentralized ones do not use a payment gateway to convert fiat currencies; instead, such venues only allow the exchange of crypto assets for crypto assets.[32] Moreover, fees requested are not addressed to the platform; instead, they are given in part to the nodes that inject liquidity[33] in the system and in part to the miner for the validation of the transaction through the Proof of Work:[34] the trade and settlement take place on the respective DLT network, namely on-chain.

Decentralized platforms were born from the willingness to eliminate the vulnerabilities of centralized platforms, building genuine peer-to-peer marketplaces on-chain. In fact, decentralized exchanges do not present a central trusted party that governs transactions, which are handled by smart contracts.

This structure poses both benefits and challenges, which will be presented in Annex II. Among them, the limitation to trade only crypto-to-crypto, but also anonymity issues and the legislator's willingness to regulate them, which constitutes an open debate to date.

1.3. Custodial and Non-custodial Wallets

Regarding the custody, safekeeping, and transfer of digital assets, users adopt digital wallets, which consist of hardware or software that hold crypto assets.

Wallets are represented by a public and a private key which are used to identify users in the blockchain and to interact with the distributed ledger performing transactions.

[32] Users are required to exchange first fiat currencies for digital assets, and then they may use the digital assets they own to exchange them with other digital assets in a DEX.

[33] Nodes injecting liquidity in the liquidity pool are rewarded either in crypto assets or in fractions of trading fees.

[34] The Proof of Work is one of the consensus mechanisms used in DLT environments. It requires the blockchain participants, namely the nodes, to repeatedly participate to computational challenges to approve and verify transactions. Participants in this process compete against each other to be the first to complete transactions and consequently get rewarded, usually with a fraction of the native asset.

The public key corresponds to the *wallet's address*, and as its name suggests, it is public. It can be considered the *IBAN* for a bank account and is used to receive crypto assets and encrypt outbound transaction information. Instead, the private key is used by the wallet owner to approve transactions and prove the ownership of the wallet's funds, representing the user's signature. This is, in fact, the reason why it must remain private, as any person other than the owner gaining access to it can take control of the wallet and, consequently, of the assets it contains, managing to move them elsewhere. The two keys are thus used in combination to perform transactions involving different wallets.[35]

Custodial and Non-Custodial Wallets' main difference is linked to who controls the private keys.

Custodial Wallets are a feature of Centralized Exchanges and are embedded in the platform. This is the main reason why the hosted (Custodial) wallet makes centralized exchanges user-friendly, provided that users are not in possession of their private key, benefitting from a lower responsibility. In fact, transferring crypto assets to another wallet only requires users to log in to the platform using their credentials and the public key representing the destination wallet.[36]

Non-custodial wallets instead impose a certain degree of responsibility on the user, who is in control of the private key. This is one of the reasons why non-custodial wallets may not be as user-friendly as their custodial counterparties. This implies the user is charged with much more responsibility since, in the case in which the private key is lost, the wallet and its content are irretrievable. Non-Custodial Wallets are used in combination with Decentralized Exchanges.

[35] Where the two keys are correctly inserted, and the beneficiary public address is provided, the wallet transmits the transaction to the network and makes the transfer effective.
[36] Then the exchange provides the private key itself and completes the transaction.

Chapter II: Opportunities and Risks

Crypto exchange platforms or in general providers of services in relation to crypto assets present both opportunities and risks. Both of them are often associated to the underlying technology as well as to the construction of platforms and the assets exchanged therein.

2.1. Opportunities

New technologies are introducing changes in the financial industry and opening up consumers and firms to new ways of accessing finance. In the same way, providers in FinTech[37] are increasingly looking for innovative solutions for citizens, with the aim to enter the market.

One of the main opportunities spotted by providers is that of granting better access to finance, with the consequent increase in financial inclusion worldwide, allowing citizens to connect and exchange assets. For example, crypto assets and their providers may facilitate micro-payments, the international transfer of remittances, and they may support financial inclusion in under- and un-banked countries.

In the European Union, FinTech initiatives are supporting operational efficiency and increasing the competitiveness of the European economy with respect to that of other countries and regions. Moreover, FinTech is playing an essential role in the Capital Markets Union,[38] introducing digitalization in existing and new business models and imposing data-driven solutions, especially regarding asset management and investment intermediation.[39]

[37] The Financial Stability Board defines FinTech as "technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services". It was the first institution to provide a definition back in 2014.

[38] The capital markets union (CMU) is a plan to create a single market for capital, thanks to which consumers, investors, and businesses can benefit from investments and savings flowing across the EU.

[39] See European Commission "Communication to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of

The financial sector[40] is grasping and exploiting more than others the opportunities provided by digitalization, among which, as introduced in the previous chapter, Distributed Ledger Technologies and Cryptography, which, used in combination, allow for the protection, integrity, and immutability of information, which is available to everyone.

Hence, as reported in the Digital Finance Strategy text,[41] "crypto-assets and their associated blockchains can bring significant opportunities in finance: potentially cheap and fast payments, especially for cross-border and international transactions, new funding possibilities for SMEs[42] and more efficient capital markets. Utility tokens can serve as enablers of decentralised blockchain networks and stablecoins can underpin machine-to-machine payments in mobility, energy and manufacturing sectors".

Experts are working on improving DLTs, primarily in relation to operational resilience, as such technology has the potential to introduce significant benefits for users once it will be able to be resilient to cyber-attacks, scalable, ensure continuity and accessibility in their services, and present sound governance.

DLT-based solutions create complex ecosystems composed of regulated financial intermediaries, technology providers, final users, and other operators. New solutions are leading to a major turning point that will transform the way information and assets are exchanged and accessed and will become a key component of the economy.

The financial sector is particularly prone to explore blockchain potential in payments, securities, deposits, capital raising, trading, and post-trading, with crypto assets representing its primary application. The Financial Stability Board, beneath the potential financial stability risks associated with crypto assets, recognizes the benefits DLT may

Regions on a FinTech Action plan: For a more competitive and innovative European financial sector", COM (2018) 109 final.

[40] Such technology can be exploited in any sector, for example, in the administrative and healthcare system.

[41] European Commission Digital Finance Strategy, page 9.

[42] Small and Medium Enterprises hardly manage to raise capital through the traditional channels; in this regard, FinTech initiatives (e.g., crowdfunding platforms, ICOs) may better channel resources from those in surplus of money to those in need of money, also providing fast and effective means to raise money from a diverse investor base, thus representing a useful alternative funding source.

provide for the future of finance. The FSB declares in fact that DLT may have applications for, among other things, securities settlement, asset registers, trade reporting, and financial inclusion.[43]

Another positive aspect is linked to the fact that Exchanges are essentially providing their services online through digital interfaces, making them an innovative and more interesting business for consumers, and introducing a new way to meet the demand and supply of assets. Furthermore, crypto assets service providers may contribute to fostering competition and enhancing the Single Market, providing a new and better user experience and promoting financial inclusion.

Although intermediaries and assets in the crypto landscape often fall outside the regulatory perimeter (as will be explained), intermediaries are increasingly expressing their willingness[44] to be part of the regulatory regime, enhancing their credibility and, above all, enjoying the possibility to scale up their businesses and provide their services at a European level through the opportunity to passport to 27 Member States and not having to adapt to a vast variety of laws.

Some initiatives are still under development, while others have already been applied. For example, after the European Commission Report on the assessment of the risks of money laundering and terrorist financing was published[45], the European Regulator extended the scope of the Anti-Money Laundering and Counter-Terrorist Financing Directive to *Virtual Assets Service Providers* and *Wallet Providers* as well.[46]

2.2. Risks

The primary risks in the crypto asset market are in part the same characterizing the traditional financial market, although presenting some unique features based on the underlying technology. They can be summarized as technological and operational risk,

[43] Financial Stability Board Report "Crypto-asset markets Potential channels for future financial stability implications", October 2018, page 4.
[44] For example, read "CZ FAQ 5 - Why Binance Embraces Regulations", Binance Blog (July 2022), in which Chapeng Zao expresses his willingness for a good regulatory regime for exchanges.
[45] SeeWhich identified virtual currencies and the related service providers as posing high risks for money laundering and terrorist financing
[46] See Chapter 3.

market liquidity risk, volatility risk, and leverage risk. Such risks represent a threat to consumers and investors, as often specified by Authorities' Warnings[47] to consumers.

The technological and operational risks are mainly related to the specific services provided within the platform and to their online nature.

For example, wallet providers or, in general, exchanges that also provide digital wallet services may present vulnerabilities concerning the protection of private keys. As mentioned in the previous chapter, users interact with the blockchain through a wallet, which entails the existence of public and private keys.

In the case of decentralized exchanges, it is the user's responsibility[48] to take care of their own private key and act with diligence to keep it secret; conversely, centralized exchanges take responsibility and control of the private keys, creating a straightforward solution for end-users.

However, this also creates an additional layer of risk, making such exchanges prone to hacks, after which users may not be able to retrieve access to their wallet again, including its content.[49]

In fact, as highlighted by "ESAs Call for Advice on digital finance and related issues" [50] of February 2021, platform infrastructures that collect and store vast amounts of personal and financial consumer data represent an attractive target for cyber-attacks,[51] increasing the risk to operational resilience.

[47] Provided by International bodies, European Agencies, and National Competent Authorities. For example, the ESAs issued warnings on the risks of crypto assets respectively in 2013, 2018, 2021, 2022.

[48] The user shall not communicate the private key to anyone nor lose it: once lost the content of the wallet would not be redeemable. Thus, a disadvantage related to DEX and private keys lies in enhanced responsibility on the user side.

[49] In the past, a number of trading platforms have collapsed after cyber incidents, leaving their customers with real losses. A famous example is the above-mentioned Mt. Gox, once the world's largest bitcoin trading platform, which collapsed into bankruptcy in Japan, leaving nearly 25,000 customers waiting for compensation.

[50] "Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities".

[51] Some notable examples include hacking thefts to Coincheck in 2018 and to KuCoin in 2019.

That said, as reported in the IOSCO Final Report[52] "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", considerations should be made concerning the safeguards to participants' assets.

When participants' wallets are hosted and controlled by the exchanges, providers also have the power to control private keys and thus all custody-related functions, including the transfer of crypto assets among participants and in or out of the platform. An example is that of Binance and Celsius *withdrawals suspension* in June 2022, which proved that when exchanges control private keys, end-users may not be able to compute transactions as they want;[53] this is the reason why it is common to say, "Not your keys, not your coins".

Exchanges may also face liquidity risks, meaning they might not be able to meet sudden withdrawal demands due to insufficient assets available to cover participants' claims or unfavorable market conditions.

Thirdly, crypto assets are particularly prone to volatility, especially when they are not backed by any contractual claim. High volatility may raise several concerns, particularly for investors, who may not be prepared to experience quick boom/bust cycles.

Finally, as with any financial asset, positions in crypto assets can present more significant risks to holders and their creditors when they involve leverage.

It is understood that, of course, one of the primary risk crypto exchanges yield, arises from the very assets they exchange: crypto assets.

Crypto assets represent one of the major applications of distributed ledger technologies in the financial field. The Financial Stability Board defines them as "a type of private digital asset that depends primarily on cryptography and distributed ledger or similar

[52]IOSCO Final Report "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms", page 12 and following.

[53] Sanctions imposed to Russia regard crypto assets too, and exchanges were required to hinder the transactions to Russian wallets. In this regard see Annex III on "A New Definition of Financial Instrument". Moreover, in June, some exchanges among which Binance and Celsius suspended Bitcoin withdrawals. In this regard see also CoinDesk articles "Binance Resumes Bitcoin Withdrawals After Pause", "Crypto Lending Service Celsius Pauses Withdrawals, Citing 'Extreme Market Conditions'", "The "Opening remarks by Commissioner McGuinness at the ECON Committee Structured Dialogue".

technology".[54] They are not of a unique kind:[55] among them, cryptocurrencies, stablecoins, and other digital tokens whose market is constantly evolving and growing.

They are associated with some risks, particularly the risks to financial stability and to investors and consumers.

The risk to financial stability is caused by the interconnectedness of the crypto asset market with the traditional financial system. It remained limited till 2021 but is currently increasing, mainly through expanded portfolios or ancillary services associated with digital assets such as custody and trading services. According to the *ECB Financial Stability Review 2022*,[56] some major payment networks favored the accessibility of crypto assets services to consumers and businesses, favoring the connection of the two markets.

In June 2022, the Bank of Italy published a communication[57] reporting the risks from the crypto ecosystem, both in terms of their relationship with regulated financial entities and those operating in decentralized environments.

The communication highlights increased interconnectedness between regulated and unregulated financial intermediaries and the lack of arrangements aimed at minimizing the effects of possible downside events. This is attributed to the fact that crypto assets and the related service providers are largely unregulated and thus pose risks to the financial system.

A survey conducted as part of the *ECB Financial Stability Review 2022* reported that institutional investors[58] are now largely investing in crypto assets, and asset managers are increasingly involved in crypto as a consequence of a major demand for this new asset class from their clients.

---

[54] Financial Stability Board "Final Report and High-Level Recommendations Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements", October 2020, page 5.
[55] Crypto assets vary in the rights they confer and in the uses they promise.
[56] European Central Bank "Financial Stability Review 2022", May 2022. Available at: https://www.ecb.europa.eu/pub/financial-stability/fsr/html/ecb.fsr202205~f207f46ea0.en.html
[57] Banca d'Italia "Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività", June 2022.
[58] Among them hedge funds and non-financial firms.

In fact, the Survey[59] highlights that, as of 2020, 56% of European institutional investors confirmed they were exposed to digital assets up to 45%. This is because products such as crypto-based derivatives and securities on regulated exchanges, such as futures, exchange-traded notes, and exchange-traded funds, are increasingly available and getting popular both in Europe and in the United States. However, the European crypto-asset management landscape remains limited, and only 20% present a home primary office location.

As far as retail investors are concerned, they represent a significant part of the crypto investor base. The ECB's *Consumer Expectation Survey*[60] indicates that 10% of households hold crypto assets. The survey highlighted U-shaped income quintiles proving a higher correlation between higher income and lower income households and detention[61] of crypto assets holding.[62] This implies that low-income individuals are prone to invest in crypto assets, although their financial position may not be resilient enough.

According to the Authorities, crypto assets do not present consumer rights and protections such as complaints procedures or recourse mechanisms, are deemed to be of high complexity and are often characterized by misleading information, as well as widely used in frauds and malicious activities such as money laundering and cyber-crime.[63]

Notwithstanding the risks, investors keep demanding such assets. Common reasons are, for instance, the perception of quick and easy gains, the innovation that characterizes such assets when compared to traditional ones, and the perception of portfolio diversification.

---

[59] See L. Hermans, A. Ianiro, U. Kochanska, V.M. Törmälehto, A. van der Kraaij and J.M. Vendrell Simón, "ECB Financial Stability Review - Decrypting financial stability risks in crypto-asset markets". Paragraph 2, "Market developments in recent years". *Survey conducted by Fidelity Digital Assets.*

[60] Whose results are reported in the ECB Financial Stability Review, Ibid.

[61] Middle-income households are less prone to hold crypto assets with respect to low and high-income ones.

[62] In this regard see Fabio Panetta's Speech "For a few cryptos more: the Wild West of crypto finance". April 2022, Columbia University.

[63] ESAs Warnings, available at: https://www.eba.europa.eu/eu-financial-regulators-warn-consumers-risks-crypto-assets.

Nowadays, crypto assets represent less than 1% of the global financial system but are still growing significantly; however, they are the same size as the securitized subprime mortgage markets that triggered the global financial crisis.[64]

Going back to the European Supervisory Agencies' opinion, they proved to be particularly concerned about consumer protection: for example, the EBA provided a list of risks[65] in relation to consumer protection arising from crypto asset service providers in its report of 2019.

Among them:

- The lack of conduct of business rules, among which risk disclosures;
- The lack of suitability checks on clients, whose risk appetite may not be sufficient for crypto-assets;
- The lack of arrangements for the management and mitigation of risks, included those related to operational resilience and cyber-security;
- Inappropriate arrangements for the segregation of assets; [66]
- The lack of rules for the prevention and mitigation of conflicts of interest;
- Inadequate advertising rules which may lead to misleading marketing communications on crypto assets;
- The lack of compensation schemes to protect customers;
- The lack of complaints handling procedures;
- The lack of a legal framework aiming at determining the parties' rights and obligations.

Several risks emerging from exchange platforms are instead linked to the very nature of crypto assets. This can be clearly seen in the numerous ESAs joint warnings, opinions, and advices on crypto assets as well.[67]

[64] FSB Report, "Crypto-asset markets Potential channels for future financial stability implications".
[65] European Banking Authority "Report with advice for the European Commission on crypto-assets" (January 2019) page 16, Box 4.
[66] Consumers' assets should be properly separated from those belonging to the firm; however, this is also tied to a good accounting structure.
[67] See footnote 63.

The European Supervisory Agencies and Central Banks[68] conveyed that crypto assets pose risks regarding investor protection and market integrity, declaring that they are, by their nature, highly risky and speculative, and therefore are not considered a viable investment or payment option for most retail investors, as most of them would not be able to bear the losses attached to them, which could even amount to the entire sum of money invested. Additionally, they remarked that crypto assets might expose consumers[69] to scams and cyber-attacks, for which they do not enjoy any protection right.[70]

However, not only is user protection at stake, but also prudential aspects of platforms are not adequately addressed. This is why the European Commission committed to providing an ad hoc regime for crypto assets service providers, which are only partially regulated today.[71]

In fact, many of the above-mentioned risks may be reduced once a clear regulatory framework is set up: this raises the risk related to the lack of proper regulation and supervision.

The absence of regulation, as reported by the Italian Agency for Securities and Financial Markets (CONSOB)[72] makes it impossible for users to be properly protected, in particular when compared to regulated financial intermediaries, for which suitability checks and internal controls, among others, are compulsory.

The IOSCO highlighted some key considerations in relation to crypto trading platforms, and in particular in relation to their access. In fact, due to the online nature of such services, access may be non-intermediated, raising concerns as regards the onboarding

[68] EBA, ESMA and EIOPA as well as central banks and national supervisory authorities. See again June 2022 "Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività" (footnote 57).
[69] For instance, the last ESAs initiative (March 2022) "#BeCryptoAware" to promote awareness about the risks of crypto assets, especially among young people who might be underestimating them. The initiative was promoted via social media and sends back to ESAs warnings.
[70] The ESAs then report the key risks from crypto assets, which were in part reported formerly. They are *volatility risk*, *misleading advertisement*, *lack of protection*, *product complexity*, *exposure to scams and malicious activities*, *market manipulation*, *lack of transparency*, and *low liquidity*, *hacks*, *operational resilience,* and *security issues*.
[71] That will be described in Chapters III and IV.
[72] See CONSOB, "Le Criptovalute".

process, which reveals to be essential both for the prevention of illegal activities and the suitability and eligibility of consumers, whose risk appetite and financial conditions should always be assessed.

In addition to potential financial stability concerns, risks to consumers, and market integrity, the risk that illicit activities are computed via exchanges and crypto assets is vivid. For example, authorities underline the presence of a high risk of money laundering and terrorist financing, sanctions evasion, fraud, tax evasion, and the circumvention of capital controls. Such risks are exacerbated by the cross-border nature of providers of crypto asset services, which makes them attractive to persons undertaking illicit activities.[73]

This will be treated in the next paragraph, dedicated to the risk of money laundering via exchanges.

2.3. Risk of Money Laundering and Terrorist Financing

New technologies, products, and services have the potential to spur financial innovation as well as improve financial integration. However, they also provide criminals with additional opportunities to launder their proceeds and finance illicit activities.

A study[74] conducted on the use of cryptocurrencies to finance illegal activities highlighted that *as of 2017*, illegal activity accounts for a substantial proportion of the users and trading activity; the authors reported that one-quarter of users and almost half of the bitcoin transactions are associated with illegal activity, with 27 million bitcoin users[75] exploiting bitcoin for illegal activities.

Interestingly, the study highlighted that the use of bitcoin for illegal purposes varied over time, and it was subject to a reduction as a consequence of the rapid growth in

[73] See footnote 64.
[74] See S. Foley, J. R. Karlsen, T. J. Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?", The Review of Financial Studies, Volume 32, Issue 5 (May 2019), page 3 and following.
[75] Data refers to April 2017. The publication reports that users conducted 37 million transactions per year for a total value of 76 billion dollars, and collectively hold bitcoins for a value of around 7 billion dollars.

mainstream and speculative interest in bitcoin and as a consequence of the emergence of alternative cryptocurrencies that allow a higher level of opaqueness, and thus, higher suitability for illicit activities.

The *FATF's second 12-month review*[76] highlighted the increasing adoption of new tools and methods to enhance the level of anonymity and opaqueness, introducing innovative ways to perform illicit financing. These include the registration of internet domains under false or hidden identity, the use of tumblers, mixers, Anonymity Enhanced Cryptocurrencies[77] (AECs), privacy wallets, and the increased use of decentralized exchanges, among others. The review also underlined that the market for anonymity-enhancing tools is expanding, with mixers and tumblers operating as *Virtual Assets Service Providers*.

Crypto exchange platforms were often[78] the locus where laundering activities took place: the Financial Stability Board[79] highlighted that providers of services in relation to crypto assets raise considerable risks[80] to money laundering and terrorist financing and other[81] illicit activities, and in fact the EBA encouraged[82] to regulate them for Anti-Money Laundering purposes.

In fact, such risks are exceptionally high when crypto assets are transacted by entities operating outside the regulatory and supervisory perimeter. Moreover, the global nature of crypto assets and of the related service providers requires tighter international cooperation due to their distributed and cross-border nature, which makes them particularly attractive to criminals wishing to pursue illicit activities.

[76] Financial Action Task Force "FATF Second 12-month review on the revised FATF standards on virtual assets and virtual assets service providers" July 2021, pages 22 and following.
[77] AECs have been increasingly adopted in darknet markets, whereas bitcoin and fiat currencies remain preferred for settlement.
[78] According to Chainalysis, in 2019, criminals laundered around $2.8 billion in Bitcoin through cryptocurrency exchanges. See M. Orcutt, "Criminals laundered $2.8 billion in 2019 using crypto exchanges, finds a new analysis", MIT Technology Review, January 2020.
[79] FSB Report, "Crypto-asset markets Potential channels for future financial stability implications", page 2.
[80] Besides those described in the previous chapter.
[81] Among which sanctions evasion, fraud, tax evasion, circumvention of capital controls
[82] See "Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849", paragraph 3.

A key point in relation to money laundering relates to the anonymity or pseudo-anonymity[83] of crypto asset transactions. In fact, although most users deem anonymity to be one of the virtues[84] of crypto assets, this can be exploited for illicit acts.[85] In general, pseudo-anonymity allows the reconstruction of transactions,[86] providing the possibility to get to the wallet address performing the operations. However, this is not happening with off-chain transactions led by centralized exchanges, which keep the balance of accounts off-chain and record on-chain crypto-for-fiat transactions only.

Unfortunately, the determinant of money laundering via exchanges lies in the soft approach to the Know Your Customer (KYC) process,[87] which can be easily overcome. This is the main reason why money laundering goes hand in hand with identity theft.[88] Therefore, excellent "Know Your Customer" and "Know Your Business" safeguards are essential for exchanges to contrast money laundering.

In fact, in general, money laundering in the crypto sector revolves around the same schemes as those used traditionally with fiat currencies, and exploits the unregulated, decentralized, and borderless networks characterizing virtual currencies. The three steps followed by criminals are placement, layering, and integration.[89]

---

[83] Anonymity translates into the ability to operate in a way that makes the operator unidentifiable whereas pseudo-anonymity implies the possibility to operate in a way in which the operator can be somehow identified while keeping their real identity protected. The blockchain groups all transactions history of currencies together with the mining of coins. The lien between the subject disposing of the crypto asset and the wallet possessor is cut, however, transactions are recorded; the process allows thus the wallet owner to remain anonym while recording the transactions and crypto assets movements on chain: this is the reason why we talk about pseudo-anonymity. The possessor of the wallet benefits from anonymity but the wallet's content is tracked.

[84] Which is derived from the trust they have in the Blockchain network

[85] See footnote 72.

[86] See Annex I on Blockchain Forensics

[87] As it only consists of a quick video or picture in which the user shows himself with their identity card.

[88] A huge number of identities is used to clean cryptocurrencies, which are fractioned and transferred through a plurality of (false) users. This is done through an exchange mixer, which increases the number of transactions so as to make it difficult to identify the fractioning.

[89] Fedor Poskriakov, Maria Chiriaeva, Christophe Cavin Lenz and Staehelin, "Cryptocurrency compliance and risks: A European KYC/AML perspective", Global Legal Insights (GLI) 2021, page 113.

First is the placement phase, in which illicit users exploit the possibility to open a high number of anonymous or pseudonymous wallets,[90] providing a low-risk opportunity for the placement of proceeds from illicit activities.

Second is the layering phase, in which the sources of funds are obfuscated through multiple transfers to different wallets, as well as the conversion of virtual assets into other virtual assets in a cross-border fashion.

Last is the integration phase, during which criminals use virtual assets for the purchase of goods or services,[91] or convert them back into fiat currency.

It follows that access to platforms becomes one of the critical issues for Anti-Money Laundering. Exchanges may provide non-intermediated access to investors, resulting in a poor onboarding process, which in turn may have consequences as regards the prevention of illicit activities on the platform, but also in relation to the investor's risk tolerance,[92] which may be overlooked. Access criteria may differ from platform to platform: some exchanges provide non-intermediated access for institutional investors, while others even to retail investors. This fragmentation brought to the IOSCO[93] advice to the regulator to ensure fair, transparent, and objective access rules for exchanges, considering proper admission criteria, which shall be chosen fairly and in a non-discriminatory fashion.

Additionally, non-intermediated access to platforms generates issues concerning the onboarding process. As opposed to regulated trading venues where the onboarding process is carried out by intermediaries[94] on behalf of their clients, crypto trading

[90] Often at no cost.
[91] The increasing availability of goods and services for which payment in crypto is accepted make the integration phase even faster.
[92] In fact, access criteria are essential for investor protection purposes and may limit participation on the platform to eligible participants and, if applicable, to participants with specific risk tolerance levels.
[93] Methodology for IOSCO, Principle 33, Key Issue 4(b) on Access Criteria states that the market and/or the regulator should: "Ensure that access to the system or exchange and to associated products is fair, transparent and objective, and consider the related admission criteria and procedures". IOSCO, "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms" February 2020, Final Report, page 10.
[94] Who in turn are responsible for KYC and AML/CFT requirements as well as the suitability assessment.

platforms may perform the onboarding process themselves. In these cases, if the process is deemed opaque or poor, this might suggest the platform is used for illicit activities. This risk may be exacerbated where the platform allows for the anonymous transfer of funds and obscures the origin or destination of the flow of funds.[95] Moreover, opaque platforms may enable participants from jurisdictions where such activities are forbidden to access as well, creating further opportunities for regulatory arbitrage.

As anticipated, such platforms may harm retail investors, which are onboarded even where the platform and products traded are not suitable according to their financial situation and attitude to risk. In this regard, IOSCO highlights a conduct principle for risk evaluation: "When establishing a business relationship with a client, a market intermediary should identify, and verify, the client's identity using reliable, independent data. A market intermediary should also obtain sufficient information to identify persons who beneficially own or control securities and, where relevant, other accounts. Procedures to implement this requirement will facilitate a market intermediary's ability to mitigate the risk of being implicated in fraud, money laundering, or terrorist financing".[96]

To this aim, a case-by-case analysis should be performed, considering single platforms peculiarities: in fact, as suggested by the FATF, a Virtual Asset Service Provider risk assessment should take into consideration the types of services offered, the products involved, transaction types, customer risk, geographical areas, and the types of currencies exchanged.[97]

As related to the last point, some considerations should be made. First, exchanges located in one jurisdiction may offer their assets and services to investors located in another jurisdiction, whose approach to anti-money laundering and counter-terrorist financing may be different. Risks from fragmentation are exacerbated where the service

[95] A survey performed by the IOSCO confirmed that most crypto asset trading platforms offer direct access to investors, including retail ones, as opposed to regulated and authorized trading venues, highlighting soft and limited anti-money laundering approaches and even absent due diligence and verification. Of course, such a gentle approach may increase the possibility that such platforms are used for illegal purposes.
[96] See footnote 93, Key Issue 11(a) of Principle 31, page 11.
[97] Back in 2020 the FATF published a report describing "red flags", namely situations that might suggest money laundering and terrorist financing activities take place on a platform.

provider is located in a jurisdiction that provides weak or nonexistent AML/CFT obligations and oversight. Hence, another consideration should be related to the level of risk characterizing the jurisdiction in which the provider is located, for example, elaborating on the level of criminal activity and the level of oversight provided by the jurisdiction.[98]

Although some risks are shared with those of traditional trading venues, in order to capture the sector-specific risks of money laundering and terrorist financing, the FATF published some risk factors in the "Updated Guidance for a risk-based approach for virtual assets and virtual assets service providers".[99]

The risk factors are reported in the form of a list, which may be helpful for authorities in the identification, assessment, and determination of the risks associated with virtual assets service providers and virtual assets, in order to mitigate them properly.

As for the Virtual Asset Service Providers, the FATF suggests considering:

- the number of VASPs for each jurisdiction and the extent to which they perform operations within the territory of that jurisdiction, including the number of transactions and the amount for each service;
- the extent to which anti-money laundering and counter-terrorist financing safeguards are applied, as well as the knowledge and repute of individuals performing those safeguards.
- The user base of the VASP and the accessibility to information by the VASP in relation to its users;
- The nature and scope of each account offered by the VASP;

[98] In relation to the above-mentioned aspects, the FATF also elaborated on the supervisory risk assessment, providing a list of categories for assessing inherent risks presented by regulated entities. They are the entity-type risk (industry, complexity of operations, business structure), customer risk (specialized product/services offered, categories of customers involved), geographic risk (both internal and international, levels of corruption and crime), products and service-related risk, delivery channel risk (customers' identification, means), and transactional risk (transaction types, flow of funds information). The list is in relation to regulated authorities, in which VASPs are included from the entry in force of the fifth amendment of the AML IV. See FATF "Risk-based Supervision", March 2021, page 20, box 2.1.

[99] See FATF "Updated Guidance for a risk-based approach for virtual assets and virtual assets service providers", October 2021, page 20.

- Eventual parameters that may lower the VASP exposure to risk, such as, limitations on the account balance;
- Whether the VASP operates online only or in person; [100]
- The level of money laundering and terrorist financing risk and the related sanctions in place associated with cross-border operations;
- Whether the travel rule[101] is implemented and whether provisions are in place for the mitigation of the sunrise issue; [102]
- Transactions involving intermediaries excluded from the list of obliged entities, and peer-to-peer transactions;
- The virtual assets offered by VASPs and their features, which may provide enhanced anonymity or enable the use of mixers or any type of service which may push obfuscation, reducing the possibility for the VASP to implement effective AML/CFT safeguards;
- The use or interaction with smart contracts.

Similarly, and to be considered in conjunction with the above list, the FATF identifies a list of features and behavior of virtual currencies which may pose a higher level of money laundering risk.

They are summarized as follows:

- The number and the amount of virtual assets transferred, its market capitalization, value and price volatility, the jurisdictions in which it circulates and the number of users per jurisdiction managing it, as well as the market share in payments in each jurisdiction; lastly, the use of the virtual asset for cross-border payments and remittances;
- The extent to which the virtual asset is exchanged with fiat currencies and for other virtual assets, and the relationship between the transactions involving the

[100] For example, trading platforms facilitating transactions between individual users or kiosk-based exchanges

[101] Which is defined by FATF Recommendation 16 on Wire Transfers as the obligation for VASPs to request and store both the originator and holder information in relation to transfers involving virtual currencies. See FATF *Updated Guidance* (footnote 99) page 57.

[102] Referred to as the lack of compliance with the travel rule by VASPs.

virtual assets through a platform and transaction of that virtual asset for fiat currencies;

- The nature and scope of the virtual asset payment channel;
- The number and value of transfers involving the virtual asset in relation to transfers relating to illicit activities (darknet marketplaces, hacking) that occur between obliged entities (among which VASPs), between obliged entities and non-obliged entities, and between non-obliged entities (namely peer-to-peer transactions);
- The use of anonymizing techniques for transfers and de-anonymizing techniques;[103]
- Exposure to Internet Protocol anonymizers, the use of which may contribute to enhanced obfuscation that prevents effective AML/CFT measures;
- The business size, customer base, and cross-border activities.[104]

However, the very fact that most virtual assets and related providers involve pseudonymous or anonymous transactions, online transactions (non-face-to-face), and payments received from unknown or unassociated third parties make them all inherently higher risk activities for money laundering and terrorist financing purposes, requiring enhanced due diligence measures.[105]

[103] Among the features that make virtual assets particularly risky from a money laundering and terrorist financing perspective is the possibility for users to compute transactions without the need of a VASP or a financial institution, their cross-border nature, which facilitates the moving of funds at a global level. Higher risk emerges when the virtual asset or the virtual asset service provider facilitates anonymity inhibiting the ability of VASPs to identify the beneficiaries of the transaction, bringing to low or absent customer and counterparty identification and consequently to difficulties in tracing the associated funds and identifying transaction counterparties.

[104] The global reach of some virtual assets and virtual assets service providers results to be a key dimension to assess a country's riskiness. Illicit users may take advantage of it for making payments or transferring funds, exploiting their transaction speed as well as the uneven supervision and oversight of financial activities involving virtual assets and the related providers.

[105] See Paragraphs 155 and 156 of the *FATF Updated Guidance* on a risk-based approach for VA and VASPs.

Chapter III: The Current Regulatory Framework

The risks characterizing the crypto asset market, together with the increasing interest from citizens, required the intervention of regulators and supervisors. As of 2021, the number of crypto assets was larger than 10.000 units, with a capitalization of 2 billion euros.[106] Following 2017, the year that marked the ICO boom, authorities started to attempt to regulate crypto assets.

3.1. An adaptation of existing rules

The first attempt to regulate the crypto assets market has been that of extending the scope of action of existing financial markets law to assets and providers, where possible. While developing tailored legislation and figuring out what were the possible implications of crypto assets and crypto assets service providers, Authorities opted for an adaptation of existing legislation that could somehow be suitable to regulate this area as well. However, as it will be explained later, most of the applicable rules regulate the asset exchanged, rather than the platform through which services are provided.

The existing regulatory framework can be divided into two main groups: preventive law and substantive law. Preventive law is adopted in order to prevent risks from materializing, requiring entities to take some precautions to diminish them and enhance the soundness of business activities. Instead, substantive law is referred to as the law that directly regulates entities per se.

As for exchange platforms and crypto assets service providers in general, at the moment there is no ad hoc European piece of law addressing them as such.

3.2. Anti-Money Laundering and Countering the Financing of Terrorism

As discussed in the previous chapter, new technologies, assets, and the services built on them have the potential to create additional opportunities for criminals to finance illicit

[106] Annunziata F., Conso A., Di Giorgio A., Lucchini A., Seri L.M., Carozzi M., Borsa P., Braccioni P., "NFT L'arte e il suo doppio – non fungible token: l'importanza delle regole oltre i confini dell'arte".

activities and launder the proceeds obtained from them. The FATF "Virtual Asset Red Flag Indicators Report for money laundering and terrorist financing risks"[107] published in September 2020, in fact, highlighted an increased use of virtual assets for money laundering and terrorist financing purposes, as well as financial sanctions evasion.

More precisely, the FATF[108] recognized that virtual assets were increasingly used in order to perform ransomware attacks, as well as proceeds-of-fraud laundering: virtual assets in fact represent a useful tool for criminals to monetize their underlying assets. The report acknowledges the main issues are related to jurisdictional arbitrage, as VASPs may be weakly compliant or even non-compliant in some jurisdictions, further enhancing the anonymity risk in virtual assets, and consequently leading to an increase in money laundering and terrorist financing risk. This, together with bad customer due diligence, makes FATF Standards application even more necessary.

The Financial Action Task Force recommends the application of a *Risk-Based-Approach* for the regulation and oversight of entities, which consists of the identification and assessment by countries and competent authorities of the jurisdiction-specific level of risk of money laundering and terrorist financing to which they are exposed, in order to adopt measures that are consistent with the level of risk identified. In so doing, the FATF promotes a certain level of flexibility, which pushes for a more efficient use of resources, allowing authorities to opt for an effective and tailored way to address the money laundering and terrorist financing risks identified during the assessment.[109]

The *Risk-Based-Approach* has been adopted for money laundering and terrorist financing purposes from the traditional financial system and is now applied to new

[107] See FATF Report "Virtual Assets Red Flags Indicators of Money Laundering and Terrorist Financing", September 2020. Offence types are, for example, the sale of illegal substances and firearms, fraud, tax evasion, computer crimes, child exploitation, human trafficking, sanctions evasion, and terrorist financing, money laundering, scams, ransomware attacks, and extortion.
[108] See FATF "Second 12-Month Review of the Revised FATF Standards on Virtual assets and Virtual Asset Service Providers" (July 2021). The review looks at the implementation of the standards from jurisdictions and the private sector, and analyses changes and developments in risks and the virtual assets market.
[109] The Risk-based Approach enables authorities to take enhanced measures to face high-risk situations or conversely to apply lighter measures where the risks are lower. See again FATF "Updated Guidance for a Risk-Based Approach for virtual assets and virtual asset service providers".

technologies as well, following the guiding principle for which *the same risks should be addressed by the same rules*.

Anti-Money Laundering and Counter-terrorist financing is tackled by the FATF from an international perspective, from the European Union from a regional perspective and by single Member States.

3.2.1. FATF Standards

At the end of 2018, the FATF amended its Recommendations in order to include in an explicit way virtual assets, as well as financial activities that involve virtual assets.

To this end, the FATF introduced a Virtual Assets (VA) and a Virtual Asset Service Provider (VASPs) definitions in the glossary, suggesting VASPs are regulated for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes, imposing them requirements as well as proper supervisory safeguards.

The FATF added the two definitions in order to broaden the boundary within which the standards should be applied, covering new types of assets and their providers, which would then be part of the list of obliged entities.

The definitions proposed by the FATF are the following:

- "Virtual asset means a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations"[110]

[110] Ibid, page 21. It can be noticed that the FATF definition of virtual assets entails a functional approach, underlying the possible uses.

- "Virtual asset service provider is any natural or legal person[111] who is not covered elsewhere under the Recommendations and as a business[112] conducts one or more of the following activities or operations for or on behalf[113] of another natural or legal person:
    i. Exchange between virtual assets and fiat currencies;
    ii. Exchange between one or more forms of virtual assets;
    iii. Transfer of virtual assets; and
    iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
    v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."[114]

The FATF specifies that both definitions should be interpreted in a *broad manner*, so as to embrace further developments and advancements, as well as granting technological neutrality.[115] However, even though they are meant to be of broad interpretation, it is specified that in order to be covered by the above definition, virtual assets must be *digital* and must be *digitally traded*, *transferred*, and be *suitable for payment* and *investment purposes*.[116]

[111] The person can be either a legal person, such as a company, or a natural person, namely an individual. It excludes those participants that do not provide or actively facilitate any of the activities that follow (such as Internet providers).
[112] The wording "as a business" excludes those performing the services or activities on an occasional basis. Entities covered are meant to carry out the function(s) on at least a sufficiently regular basis and for commercial reasons.
[113] The wording "for or on behalf of another natural or legal person" is meant to exclude those performing the business for themselves as well as the internal transfer of virtual assets by a single legal person within that legal person. Services should be performed for or on behalf of third parties, which may be, for example, users or customers.
[114] See FATF *Updated Guidance*, (footnote 109), page 22.
[115] Technological neutrality stands for the application of standards, in this case to virtual assets, irrespectively to their underlying technology but instead with a focus on their basic characteristics.
[116] This means virtual assets definition covers numerous activities, such as the simple transfer of the asset to another person or on behalf of others, the change of ownership, the destruction of the asset as well as the mere exchange of the asset for something else.

Nevertheless, the legal characterization of assets lies at the base of proper risk mitigation and management[117] as will be clarified later.

The FATF precises that also the definition of VASPs is intended to be interpreted broadly, and that VASPs should be identified as such irrespectively of their names, but instead in relation to the services and activities they offer; once they perform services that fall within the above definition, they shall be treated as such.[118]

The FATF also specifies the individual functions of VASPs, so as to clarify the definition provided.

- "Exchange between virtual assets and fiat currencies" refers to the exchange of any virtual asset for fiat currencies and vice versa.
- "Exchange between one or more forms of virtual assets" relates to the exchange of virtual assets for virtual assets, meaning that one kind of virtual asset is used as a form of payment to get a different virtual asset.[119]
- "Transfer of virtual assets" means any service allowing for the transfer of ownership or control[120] of a virtual asset either to another user or to another address held by the same user. The mere activity of transferring a virtual asset from one address to another on behalf of another natural legal person and irrespectively of the fact that the parties involved in the transaction coincide or not, would be covered by this definition.[121]

[117] In fact, jurisdictions should take in consideration the specific usages assets (whether it is used for payment or investment purposes), which may vary from country to country. Moreover, they should assess whether there exist a suitable regulatory regime for them. Should a jurisdiction choose to define a virtual asset as a financial asset, existing AML/CFT standards and financial assets regulations would apply.

[118] The FATF precises that in order to avoid any overlap, the VASP definition applies to entities not falling under other definitions provided in the Recommendations; for example, financial institutions are not covered.

[119] *The Guidance* specifies that in order to qualify as a VASP, an entity does not necessarily have to provide both fiat-to-crypto and crypto-to-crypto exchange services, as long as it conducts the exchange activity as a business and on behalf of another natural or legal person.

[120] A transfer takes place when a new party takes custody or ownership of a virtual asset or has the possibility to benefit from that. This includes transfers among users of the same VASP too, including where VASPs record transfers off-chain. This service includes, for example, the facilitation of users to transfer virtual assets to other individuals.

[121] Other services or business models in relation to virtual assets may constitute exchange or transfer activities based on the first three listed activities present in the VASP definition, provided the VASP exercises them for or on behalf of a third party. They are, for example, virtual

- "Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets" is intended as an entity having control over a virtual asset. Safekeeping consists in holding virtual assets on behalf of another person or exercising control over the private keys. Instead, the administration stands for the management of virtual assets on behalf of another person. As for control, it consists of the ability to hold, trade, transfer or spend the virtual asset, change its disposition or use it.[122]
- "Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset" covers Initial Coin Offerings-related activities. It consists in the participation or provision of financial services related to the offer or sale of virtual assets as a consequence of an ICO.[123] The mere activity of issuing a virtual asset does not fall within this definition: the creation act without the performance of any activity on behalf of a natural or legal person does not, in fact, make the creator a VASP.

Anti-Money Laundering and Counter-Financing of Terrorism regulations are supposed to be applied to virtual assets and virtual assets service providers irrespective of the activity type(s) they carry, their underlying technology, and eventual additional services performed.

Once established the definition of Virtual Asset Service Providers, their duties and obligations are determined too. In particular, being subject to anti-money laundering requirements entails the performance of Customer Due Diligence, Record Keeping, and Suspicious Transactions Reporting.

Customer Due Diligence (CDD) is a process whose ultimate goal is to help obliged entities, among which VASPs, assessing money laundering and terrorist financing risks.

---

assets escrow services, brokerage services, order-book exchange services, and advanced trading services as well as exchanges or transfer services that facilitate the exchange of virtual assets for fiat currencies.

[122] See *FATF Updated Guidance*, VASPs Individual Functions. Safekeeping and administration services include persons controlling another person's private key. This activity is often performed with others, (from the above list) as natural or legal persons involved in safekeeping and administration are likely to perform exchange and transfer services.

[123] See *FATF Updated Guidance*, VASPs Individual Functions. For example, this could include book building, underwriting, market making, and placement agent activity.

More precisely, it encompasses client identification, which typically includes the customer's name and other information such as their physical address, date of birth, and a unique national identifier number. In general, the CDD process requires VASPs to collect further information for the verification of customer identity, as well as for determining their risk attitude and financial situation. Among them, VASPs should demand the IP address with an associated time stamp, geo-location data, device identifiers, digital wallet addresses, and transaction hashes.

VASPs are required to avoid entering into a business relationship or perform occasional transactions on behalf of users on which the above information is not collected, and report them for suspicious transactions instead.

The CDD measures should also allow the VASP to create a customer profile, which would enable them to perform ongoing due diligence and support the VASP in the decision to *enter, continue, or terminate* a business relationship.

A key role of the CDD process is also that of understanding the true purpose and nature of the business relationships. VASPs can thus open and maintain accounts,[124] provided that they collected the relevant information for money laundering and terrorist financing purposes when their activity is that of providing a service on behalf of their clients. Moreover, when a VASP performs an occasional transaction[125] that amounts to a threshold higher than USD/EUR 1000 it shall perform CDD either way.[126]

To this aim, a well-established and effective procedure for the identification and verification of clients' identities on a risk basis is essential regardless of the nature of the transaction, whether it is occasional or not.

Of course, this must be performed in compliance with the Risk-Based Approach,[127] as countries may present different characteristics with respect to money laundering and terrorist financing, and given the cross-border features, anonymity, and obfuscation

[124] Namely establishing a relationship

[125] Which is not defined as an established and continued relationship as in the first case

[126] As reported in *Recommendation 10* of the FATF "Updated Guidance on virtual assets and virtual asset service providers", page 7. However, as provided in paragraph 152, page 49, jurisdictions may require the performance of CDD also for transfers or transactions, including those "occasional" also for amounts lower than USD/EUR 1000.

[127] Justified by the country's assessment of risks, namely the identification of higher risks.

potential of virtual assets, countries may choose to have a more stringent approach with respect to CDD, for example by lowering the threshold for which CDD is required for occasional transactions[128] to less than USD/EUR 1000.

In fact, some circumstances require enhanced[129] CDD measures due to higher ML/TF risk, which can be linked, for example, to a specific geographical area.

Among them:

- Countries or geographic areas which are recognized by supranational bodies to be inclined to terrorist funding or support provision or having terrorist organizations operating within them;
- Countries characterized by notable levels of organized crime, corruption, or other criminal activity (such as illegal drugs sources or transit, human trafficking, smuggling);
- Countries subject to sanctions, embargoes, or any other measure issued by international organizations such as the United Nations;
- Countries characterized by weak governance or regulatory regimes, poor law enforcement, and a soft or absent approach to AML/CFT, especially for VASPs.

Of course, VASPs and other obliged entities are also required to check on their clients on a regular basis, performing ongoing CDD in order to ensure data are revised,[130] and understand whether their clients' transactions are consistent with their profile and expected behavior. Monitoring is also essential in order to spot potentially suspicious transactions[131] for money laundering and terrorist financing purposes.

[128] See footnote 126. As reported in Recommendation 10, jurisdictions should be able to assess how VASPs identify and determine that transactions are conducted on an occasional basis rather than on a continuous basis.

[129] VASPs located in, or virtual assets transfers from or associated with particular countries may potentially present higher risks to money laundering and terrorist financing.

[130] Ongoing CDD is particularly important for higher-risk customers or categories of virtual assets products or services; in general transactions and record reviews are essential also for compliance with the travel rule.

[131] For example, transactions that do not fit the expected client's profile behavior, or that deviate from their usual pattern of transactions may be potentially suspicious.

As for Record-keeping purposes, the FATF also recommends that VASPs keep all transaction records and the related information[132] for a period of five years, so as to be able to reconstruct transactions' history and detect suspicious ones, and eventually send relevant information to competent authorities.

Countries should require VASPs and other obliged entities providing services in relation to virtual assets to perform AML/CFT safeguards irrespective of the entities' operational model, technological tools, ledger design, or any other operating feature.[133]

3.2.2. Anti-Money Laundering and Counter-Terrorist Financing in the European Law

Virtual assets service providers are directly addressed by the *anti-money laundering and countering the financing of terrorism legislation*.[134] *Directive EU-2015/849* incorporates some of the Financial Action Task Force Recommendations,[135] and requires exchanges and wallet providers to perform anti-money laundering and counter-terrorist financing safeguards.

From a European Law perspective, Crypto assets service providers are directly addressed by the anti-money laundering and counter-terrorism financing legislation,[136] regulated by Directive 2015/849. The current version in force is the fifth AML/CFT Directive,[137] which should be read in conjunction with[138] the Transfer of Funds Regulation, and comes as an amendment to the fourth AML/CFT Directive.

---

[132] Namely information on the relevant parties, including their public keys, the accounts involved, the nature and date of the transaction, and the amount transferred.
[133] However, the entity is subject to them only where it provides a qualifying service.
[134] See European Commission "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC".
[135] See again FATF "Updated Guidance" (Footnote 109).
[136] The first anti-money laundering Directive was adopted by the EU in 1990 in order to prevent actors to use the financial system for money laundering purposes. The Directive has been continuously revised to capture emerging money laundering and terrorist financing risks.
[137] See Footnote 134.
[138] The AML/CFT and TFR should be read in conjunction; they both take into account the FATF Recommendations.

In drafting the Directive, the European Commission took into account the FATF Recommendations in relation to money laundering and terrorist financing risks. Similarly to the FATF Updated Guidance on a Risk-based approach, the fifth AML/CFT introduces the definition of *virtual currency* as follows:

"Virtual currencies means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically". [139]

Interestingly enough, differently from the definition provided by the FATF GAFI, it can be noticed that the AML/CFT refers to "virtual currencies" rather than to "virtual assets". The reason is that the AML/CFT Directive is focused on the description of the virtual currency as opposed to that provided by the FATF, which adopts a more functional approach. This can be inferred from the wording "digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes", as opposed to the AML/CFT definition provided above, whose aim is to declare what a virtual currency is (or is not).

The "virtual currency" definition context is not as broad as the one conveyed in the "virtual asset" one, highlighting that the regulator's aim was in fact to regulate "cryptocurrencies", which may be currently classified only as a subset of crypto assets.

On the other hand, for what concerns Providers, the Directive does not propose a broader definition with respect to that of the FATF; however, it adds the definition of *custodian wallet provider* to which anti-money laundering safeguards are extended too.

In fact, Article 3 of the Directive defines "custodian wallet provider" as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies".

To make the application of the Directive clear, the legislator provided a list of *Obliged Entities*, namely a list of legal persons whose obligation is to perform anti-money

[139] See Article 3, Recital 18 of Directive (EU) 2015/849.

laundering and counter-terrorist financing safeguards: with the 2018 amendment, *virtual currency exchange platforms* as well as *custodian wallet providers* are added as follows:

"(g) providers engaged in exchange services between virtual currencies and fiat currencies;

(h) custodian wallet providers".[140]

As a consequence, providers that engage in exchange services between virtual currencies and fiat currencies, the so-called "gatekeepers", and custodian wallet providers are subject to AML/CFT requirements, provided that the underlying assets fall under the AMLD V definition of virtual currencies.[141]

From a practical perspective, this implies that they are required to perform Customer Due Diligence (CDD)[142] as reported in Art. 13 and following of the Directive as a foundation of the Know Your Customer (KYC) process, which requires entities to define their clients' profiles and understand their financial behavior, as well as the kind of money laundering or terrorism financing risk they pose. Moreover, obliged entities shall

[140] Article 2, points g and h, *Directive (EU) 2018/843*. The Action Plan to strengthen the fight against ML/TF which lays at the base of the AML describes Virtual currency exchange platforms as "electronic currency exchange offices that trade virtual currencies for fiat currencies. Virtual currency wallet providers hold virtual currency accounts on behalf of their customers. In the 'virtual currency' world, they are the equivalent of a bank offering a current account on which fiat money can be deposited. They store virtual currencies and allow for their transfers to other wallets/virtual currency accounts". The fifth AML/CFT directive clarifies that virtual currencies should not be confused with electronic money, which instead is defined in the E-Money Directive (*Directive 2009/110/EC*) as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer".

[141] Interestingly, as reported by Poskriakov, Chiriaeva, Lenz, and Staehelin in the 2021 edition of the Global Legal Insights on Blockchain and Cryptocurrency Regulation, page 116, most crypto-to-fiat (or fiat-to-crypto) exchanges are considered obliged entities; nevertheless, crypto-to-crypto exchanges do not seem to be expressly covered unless performed by obliged entities listed. This means that crypto-to-crypto exchanges are not per se considered obliged entities but if an obliged entity performs crypto-to-crypto exchanges in addition to another activity expressed in the list, then this activity will be covered too.

[142] Customer Due Diligence consists in the collection of all relevant information needed to properly identify a customer's identity and to better assess the level of criminal risk they present

keep track of transactions performed by their clients and submit suspicious activities to the designated National Competent Authority.

The Customer Due Diligence safeguards reported in the Directive reflect those highlighted by the FATF. Article 13 reports that obliged entities shall:

- identify the customer and verify the identity provided based on documents, data, and reliable information, with an additional secure, remote, or electronic identification;
- identify the beneficial owner and, where possible, verify their identity;
- assess the nature and purpose of the business relationship on an ongoing basis; [143]
- ensure that persons taking on transactions, and in general the business relationship on behalf of the customer, are properly authorized and identified.

Article 14 specifies that customer due diligence shall be performed "not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, or when the relevant circumstances of a customer change, or when the obliged entity has any legal duty in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owner(s)".

As stated by Article 15 of the same Directive, when a Member State or an obliged entity identifies areas of lower risk, "simplified customer due diligence measures" may be applied. Conversely, as specified by Article 18, in situations where high risk[144] is detected by the Member States, obliged entities are required to perform instead "enhanced customer due diligence measures"[145] so as to tackle those risks in an appropriate manner.

[143] The nature and purpose shall be assessed on a continuous basis, with the aim to ensure transactions undertaken are in line with the obliged entity's knowledge of the customer.
[144] A non-exhaustive list of risk situations is reported in *Annex III* of *Directive 2018/843*. The three risk areas for which examples are laid down are "Customer risk factors (e.g. the business relationship is conducted in unusual circumstances), Product, service, transaction or delivery channel risk factors (e.g. products or transactions that might favour anonymity), Geographical risk factors (e.g. countries providing funding or support for terrorist activities)".
[145] Member States shall require obliged entities to examine the background and purpose of all complex and unusually large transactions, as well as all unusual patterns of transactions. In

As regards the *Reporting Obligations*, Article 32 and following require each Member State to establish a Financial Intelligence Unit (FIU) "to prevent, detect and effectively combat money laundering and terrorist financing". FIUs are responsible for receiving and analyzing suspicious transaction reports and other information relevant to money laundering, associated predicate offenses or terrorist financing, and they can require obliged entities to provide additional information where necessary. The amendment to the fourth AML/CFT Directive improves FIUs' work by providing them with better access to information through centralized bank account registers, which also aim at strengthening cooperation among Authorities.

The 2018 amendment gives in fact Financial Intelligence Units the power to obtain the addresses and identities of owners of virtual currencies, lowering the risk associated with anonymity features characterizing cryptocurrencies.

Lastly, Article 47 requires Member States to "ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered, that currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered,[146] and that providers of gambling services are regulated".

In relation to the amendments provided to the fourth AML/CFT Directive, it shall be noted that the exchange platforms added to the obliged entities list do not seem to include, for instance, *virtual-to-virtual exchanges* or other types of services that *do not involve fiat currencies*,[147] narrowing down the subject matter compared to the services in relation to virtual currencies provided by the FATF. Interestingly, since the EBA's Opinion of 2014, services such as crypto-to-crypto exchanges have become more prevalent, raising concerns to authorities in relation to AML/CFT risks. In fact, both EBA

particular, obliged entities shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

[146] The amendment requires providers of cryptocurrency exchanges and wallets to be registered with the competent authorities in their domestic locations for AML purposes.

[147] Back in 2014, the EBA recommended bringing into the scope of the AMLD virtual currency-to-fiat exchanges and providers of virtual currency custodian wallet services in order to mitigate the risks of money laundering/the financing of terrorism arising from those activities in its Opinion "EBA Opinion on 'virtual currencies'". To this aim, legislative amendments were agreed in the context of the AMLD5 such that the above-mentioned providers were added to the 'obliged entities' list.

and ESMA agreed on the importance of the extension of the scope of the AMLD in light of the recent market developments, and to further include the recommendations of the Financial Action Task Force to cover the whole set of providers in relation to crypto assets.

3.3. MiFID

Substantive law is defined as the law that directly regulates, in this case, crypto service providers, among which crypto exchange platforms. Currently, no ad hoc European piece of law addresses them per se. Thus, as anticipated, authorities opted for an adaptation of existing law, and more specifically, the approach consists in regulating exchange platforms based on the classification of the assets they allow to trade: hence, regulating the facility in which they are exchanged would then be a consequence of the legal nature of exchanged assets.

For this purpose, the most relevant piece of legislation is the Markets in Financial Instruments Directive II (MiFID II).[148]

However, as anticipated, in order to understand whether the crypto exchange platform should be subject[149] to MiFID II, a case-by-case analysis should be made based on the outcome of an attentive legal classification of the assets exchanged.[150]

[148] European Commission "Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU".
[149] Namely considered a trading venue for MiFID purposes.
[150] The existing legal framework may be applicable to crypto assets trading platforms in secondary markets depending on the assets' nature.

Crypto assets shall be classified according to their legal nature, and more precisely, as was first suggested by the FINMA ICO guidelines[151] back in 2018, we shall distinguish four types[152] of crypto assets:

- *Utility tokens* - which allow users to perform determined activities in a digital infrastructure. They provide the right of ownership of the token itself and additional rights such as access to some goods or services.
- *Payment tokens* - which are intended to be used as a means of payment for the purchase of goods or services or as a means of money or value transfer; they correspond to cryptocurrencies. They provide the ownership right of the token.[153]
- *Investment tokens* - representing a debt or equity claim on the issuer. They are called security tokens since they share the same characteristics of equity, debt, and derivative instruments. They are in fact tied to an underlying physical asset[154] and may entitle their owner to the right of future cash flows. This category is also comprehensive of tokens that allow a physical asset to be traded on the blockchain.
- *Hybrid tokens* – tokens sharing some features of more than one of the above-mentioned token types. For example, asset and utility tokens can also present characteristics that would be attributed to payment tokens as well.[155]

[151] The Swiss Financial Market Supervisory Authority (FINMA) was the first one to define an approach on how to apply financial market legislation to crypto assets and in particular to ICOs in the document "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)" (February 2018). The approach comes as a guideline in which the authority clarifies the principles upon which it bases its responses to inquiries.

[152] This approach is defined as a bottom-up approach as the classification of tokens is performed based on the analysis of their characteristics. See F. Annunziata, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", page 38.

[153] They are represented, for example, by Bitcoin, and, as reported in the above-mentioned paper, (footnote 152, page 23), they should fulfill the economic criteria of fiat currencies.

[154] They represent the ownership of a fraction of the value of an asset, for example of a firm, but not the ownership of the asset itself.

[155] The FINMA in this case would impose cumulative requirements – namely to treat such tokens both as securities and payment means. See again "FINMA ICO Guidelines", page 3 (footnote 151).

As mentioned earlier, utility tokens enable access to a good or service but are not accepted as a means of payment, nor entitle the owner to future profits.[156] For example, utility tokens may provide the right to access a company's services or benefits, or grant holders some governance rights. However, they are not widely accepted as a means of payment and do not promise cash flows; instead, they enable users to make a functional use of the blockchain.

Hence, they do not fall under any of the definitions provided by applicable European Financial Law and do not need to fulfill MiFID II legal requirements.[157]

Hybrid tokens present some difficulties when it comes to their taxonomy, as it is still debated. A possible solution would be that of considering weighting the features that make them hybrid and classifying them according to the one that prevails, or also regulating them in a cumulative manner.

The same cannot be said as regards Payment tokens and Investment tokens.

Payment tokens, also referred to as cryptocurrencies, can be triggered by the Electronic Money Directive[158] category of e-money. According to art. 2 of the Directive,[159] "electronic money means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer".

Thus, as provided by the European Banking Authority in the "Report with advice for the European Commission on crypto-assets",[160] if during the assessment performed by the competent authority the token satisfies the requirements of being *electronically*

[156] For example, as for cloud services, tokens may be issued with the purpose of facilitating access.
[157] Utility tokens do not reflect digitally native assets but instead depict a tokenized claim to a good or service that will be provided by the token issuer.
[158] See European Commission "Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC".
[159] Ibid
[160] EBA "Report with advice for the European Commission on crypto-assets" (January 2019), Box 3 "Crypto-assets and 'electronic money'", page 13.

stored,[161] having *monetary value*, *representing a claim on the issuer*, being *issued on receipt of funds* and for the purpose of making *payment transactions* and *being accepted by persons other than the issuer*, then, the token would be considered as E-Money under E-Money Directive.[162] Under these circumstances, authorization to operate as an electronic money institution would be triggered.[163]

Moreover, if cryptocurrencies qualify as electronic money under E-Money Directive, then they would match the definition of "funds"*[164]* proposed by the Payment Service Directive.[165] As a consequence, if a firm[166] is willing to carry out an activity falling in the payment services' list present in Annex I[167] of the PSD II (with a crypto asset that qualifies as electronic money) licensing would be triggered.[168] However, only few cryptocurrencies fall under this definition, as some of them may not satisfy the requirement of *having an issuer* as a consequence of decentralization.[169]

Investment tokens and consequently the platforms exchanging those assets may trigger MiFID II requirements in some circumstances.

[161] The EBA underlines that the definition of electronic money provided in the EMD II should cover electronic money both when it is held in a payment device (e.g. magnetic chips) or stored remotely in a server that is managed by the holder through a specific account for e-money (e-wallet). The definition is broad enough to include newly developed products too.

[162] This definition of E-money may cover stablecoins, when backed 1:1 by a legal tender and when used as a means of payment: "Stablecoins are a relatively new form of payment/exchange token that is typically asset-backed (by physical collateral or crypto-assets) or is in the form of an algorithmic stablecoin (with algorithms being used as a way to stabilise volatility in the value of the token)", ivi, page 7. In particular, they would be stablecoins having as underlying asset a fiat currency.

[163] Pursuant to Title II of the EMD2 II, unless exemptions apply in accordance with Article 9 of that Directive.

[164] See point (25) of Article 4 of Commission "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".

[165] Ibid.

[166] Whether newly established or already authorized as E-Money Institution

[167] For example, the execution of payment transactions, including issuing of payment instruments and/or acquiring payment transactions and money remittances

[168] Institutions authorized under EMD II can also perform payment services whereas payment service providers cannot issue e-money without being authorized for that specifically.

[169] As a consequence of decentralization, the issuer may not be a legal person but the community as such. In this regard, see Annex II on DeFI Regulatory Challenges.

They represent a peculiar category, for which the classical bottom-up approach for the taxonomy of tokens might be problematic, as will be described later.

MiFID II defines an Investment firm as "any legal person whose regular occupation or business is the provision of one or more investment services to third parties and/or the performance of one or more investment activities on a professional basis",[170] where the investment services and activities are listed in Annex I, section A[171] of the Directive among which "Operating of an MTF"[172] and "Operating of an OTF".[173]

In detail, the Directive states that the above-mentioned services and activities are subject to the requirements imposed *when related to Financial Instruments*, which are then reported in Annex I, Section C.[174]

Thus, what should be ascertained is whether investment tokens can be assimilated to any of the Financial Instruments presented by the MiFID, and a clear overlap may be found in particular with transferable securities.[175]

---

[170] Article 4, recital 1 of Directive 2014/65/EU

[171] Annex I Section A reports them as follows: "Reception and transmission of orders in relation to one or more financial instruments; Execution of orders on behalf of clients; Dealing on own account; Portfolio management; Investment advice; Underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis; Placing of financial instruments without a firm commitment basis; Operation of an MTF; Operation of an OTF".

[172] Article 4 paragraph 22 of Directive 2014/65/EU provides the definition of MTF as follows: "Multilateral trading facility or MTF means a multilateral system, operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments – in the system and in accordance with non-discretionary rules – in a way that results in a contract in accordance with Title II of this Directive".

[173] Article 4 paragraph 23 of Directive 2014/65/EU provides the definition of OTF as follows: "Organised trading facility or OTF means a multilateral system which is not a regulated market or an MTF and in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract in accordance with Title II of this Directive".

[174] MiFID Financial instruments are Transferable securities; Money-market instruments; Units in collective investment undertakings; Financial contracts for differences; Options, futures, swaps, forward rate agreements and any other derivative contracts; Derivative instruments for the transfer of credit risk; any other derivative contracts which have the characteristics of other derivative financial instruments, having regard to whether, inter alia, they are traded on a regulated market, OTF, or an MTF; Emission allowances consisting of any units recognized for compliance with the requirements of Directive 2003/87/EC.

[175] As discussed by Filippo Annunziata in his paper "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings", although it is unlikely that a token shares the same characteristics as "money market instruments" (Annex I,

Transferable securities are then defined as "classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:

(a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
(b) bonds or other forms of securitised debt, including depositary receipts in respect of such securities;
(c) any other security giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures".[176]

Thus, the Transferable Security definition highlights that the MiFID not only recognizes securities as Financial Instruments but also those assets sharing their characteristics, of course, satisfying the *negotiability* feature.[177]

The transferable security definition would also be comprehensive, reasonably, of financial derivatives, particularly where tokens that are classified as transferable securities or units in collective undertakings that are used as underlying in a derivative instrument.

Additionally, investment tokens that reflect an underlying pool of assets may be assimilated to units in collective investments undertakings.[178]

Where tokens cannot be qualified as transferable securities nor units in collective investment undertakings,[179] the category to be analyzed is that of derivatives, and in

Section C, (2)), some tokens might qualify as units of collective investment undertakings (CIUs) (Annex I, Section C (3)) when they reflect an underlying pool of assets.

[176] See Article 4 paragraph 44 of Directive 2014/65/EU. Tokens may offer rights to future profits and thus may be assimilated to MIFID Financial Instruments, including Transferable Securities.

[177] Albeit there are still concerns and ongoing debates on how this should be interpreted in the MiFID context. Ibid, page 40.

[178] As presented in Annex I, Section C, paragraph 3 of the MiFID II. This possibility is shared by different Member States as confirmed in the ESMA Advice on Initial Coin Offerings and Crypto-Assets (page 35, paragraphs 165 and 166) and shared by Annunziata, F. in his Paper (See footnote 175).

[179] And considering that they cannot reasonably be assimilated to money market instruments as defined in the MiFID II.

particular, commodity derivatives.[180] As outlined by F. Annunziata in his paper "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings"[181] this raises problems, as the MiFID regime regulates only commodity derivatives presenting a financial nature, the classification of which is quite complex.[182]

This is the reason why the author proposes a solution to the (sometimes) harsh classification of tokens, stating that a top-down approach would be better as, once a platform is considered as a *MiFID II trading venue*, then any asset exchanged would be considered a financial instrument and hence, requiring less effort for the identification of tokens that may be assimilated to commodity derivatives.

Considering the bottom-up approach, where a token falls under any of the definitions of the MiFID Financial Instruments, the platform in which it is exchanged would classify as a MiFID trading venue (where "trading venue means a regulated market,[183] an MTF or an OTF" [184]) and thus, be subject to the authorization[185] requirements to operate. This implies that the provider would then have to apply the organizational requirements, the conduct of business rules, and the transparency and reporting requirements laid down in the Directive.

---

[180] Defined in Annex I, Section C, paragraphs 5, 6, 7 of the MiFID as provided by the MiFIR definition of commodity derivatives in Article 2, paragraph 30.

[181] Chapter III, Subparagraph 1, "The Need to Look Beyond". See Footnote 178.

[182] The Author presents the features that make a commodity derivative "financial" in a sense. First, it considers commodity derivatives having as underlying an asset, activity, parameter, index, right or variable, the wide notion of derivatives, which includes futures, options, swaps, and any other traditional derivative but also structures, contracts, or instruments similar to the traditional ones and finally the fact that the derivative may be regulated in cash or traded on a MiFID trading venue.

[183] Article 4, Recital 21 of Directive 2014/65/EU defines Regulated market as: "Regulated market means a multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments – in the system and in accordance with its non-discretionary rules – in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is authorised and functions regularly and in accordance with Title III of this Directive".

[184] Article 4, Recital 24 of Directive 2014/65/EU.

[185] Authorization should be given by the National Competent Authority of the Member States after which it can passport (be entitled to provide the investment services or activities for which it is authorized) to other Member States without the need to seek a separate authorization host Member State.

ESMA highlights that where a token is classified as MiFID Financial Instrument and in particular as transferable security or unit in collective investment, the token would be also subject to other EU financial rules. Among them, the Prospectus Regulation, Prospectus Directive,[186] the Transparency Directive, the Market Abuse Directive, the Short Selling Regulation, the Central Securities Depositories Regulation and the Settlement Finality Directive.[187]

However, the Authority also indicated that the above-mentioned rules may present gaps, for instance leaving some issues unaddressed or, conversely, may require the application of standards that are not relevant or applicable considering the underlying technology.[188]

3.4. Legal uncertainty

The previous paragraphs highlight an attempt to regulate crypto exchange platforms and crypto assets. However, especially for what concerns MiFID II, EMD II, and PSD II, the current regulatory framework revolves around the classification of crypto assets into the standard categories provided for by the system of financial regulation that, as previously mentioned,[189] can be recognized as a "bottom-up approach".

[186] Or AIFMD/UCITS requirements if considered a collective investment unit.
[187] See ESMA "Advice on Initial Coin Offerings and Crypto-Assets" (January 2019), page 5, paragraph 7.
[188] From a more practical perspective, the ESMA elaborated on the applicability of MiFID II to crypto assets trading platforms (ibid, page 24) inasmuch they currently represent the most prevalent class of intermediaries in this market and potentially raise specific risks. ESMA identified three broad categories of platforms (which are of course not exhaustive since platforms providing different services or activities might be cut across the three categories below). They are, respectively, "(i) those that have a central order book and/or match orders under other trading models (ii) those whose activities are similar to those of brokers/dealers and (iii) those that are used to advertise buying and selling interests". The Authority thus suggests that platforms identified in point (i) should be treated as multilateral facilities and thus should comply with Title III or Title II of MiFID II as Regulated Markets, Multilateral Trading Facilities or Organised Trading Facilities. In such cases requirements are, inter alia, capital requirements, organizational requirements, investor protection safeguards, on access, on pre-and-post trade transparency, and on transaction reporting and records keeping.
[189] See footnote 175.

However, attention should be drawn to the moments following the placement phase, when assets are traded.[190] To this aim, a top-down approach may help integrate the bottom-up one, as it would instead focus on the platforms where crypto assets are exchanged, reversing the perspective.[191] Relocating the attention to the trading platform would in fact entail that the token would be covered by the MiFID, and that the trading platform would need to be authorized as a MiFID trading venue (*Regulated Market, MTF, OTF*), and carry the consequences described in the previous paragraph regarding the requirements.

The debate is still open, and the qualification of tokens and of trading venues is currently raising significantly the legal uncertainty, as remarked by the 2019 ESMA "Advice on Initial Coin Offerings and Crypto-assets".

In fact, as presented by the document and reported in the second chapter of this Thesis, one of the greatest challenges to regulators and market participants related to this field, which is relatively new and still evolving, consists in the *lack of clarity* on how the existing regulatory framework applies to crypto assets.[192]

As of now, the key consideration relates to the legal nature of crypto assets (i.e., bottom-up approach), from which in turn the applicability of financial markets law is assessed, always taking into consideration the variety of such assets and the fact that they are often framed into more than one category, so a case-by-case analysis reveals to be essential.

The ESMA Survey[193] on the qualification of crypto assets reported that the vast majority of National Competent Authorities recognized that some crypto assets[194] were to be understood as transferable securities or, in general, MiFID financial instruments.

[190] As brought up by Annunziata, F. in his paper (ibid).
[191] For example, if a token is negotiated in a MiFID Trading Venue, then the token would be automatically considered a financial instrument, irrespective of the rights it confers.
[192] If it applies, some areas may require different interpretation or should be re-considered; moreover, areas in which no regulation applies, should be then re-examined, always following the technology-neutrality principle discussed in the previous paragraphs.
[193] Back in 2018, ESMA conducted a survey to Member States' NCAs to assess the circumstances under which crypto assets are considered financial instruments. National Competent Authorities were provided with a set of existing crypto assets that reflected investment-type, utility-type, payment-type, and hybrids of the three.
[194] Especially those presenting some form of profit attached.

However, being MiFID a Directive, Member States transposed it in their jurisdiction in various ways and, for example, some of them elaborated on financial instruments in a broader manner with respect to others, which preferred a restrictive list. The consequence is that the classification of tokens becomes a matter of specific national implementation and disregards unanimity, boosting regulatory arbitrage and creating challenges for both regulators and supervisors.

In general, where crypto assets qualify as MiFID financial instruments, a number[195] of EU financial rules are likely to apply to issuers or providers; on the other hand, as far as the existing regulatory framework is concerned, some gaps and issues emerged when it applies to crypto assets. In particular, some risks[196] presented are deemed to be technology-specific and thus may be left unaddressed, raising concerns to the authorities.

Moreover, ESMA declared that although some assets may be covered by existing rules as mentioned above, most crypto assets fall outside the scope of EU financial services legislation,[197] and some exchange platforms operate outside any regulatory regime. The consequence and the major source of worry for the authorities is in fact related to investors protection, as the absence of regulation implies they are not protected in any way. Additionally, the majority of investors are not able to distinguish between regulated and unregulated crypto assets, especially when they are available for trading in the same venues, leaving them unable to choose in a conscious manner.

On the other hand, when crypto assets are classified as MiFID financial instruments, a full set of rules is applied to them and to the trading venues operating in relation to them. National Competent Authorities agree with such assessment, albeit they claim difficulties regarding the interpretation of such rules, being evident they were not designed having crypto assets in mind. Additionally, the Survey highlights that Member

[195] Inter alia, the Prospectus Directive, the Transparency Directive, MiFID II, the Market Abuse Directive, the Short Selling Regulation, the Central Securities Depositories Regulation, and the Settlement Finality Directive.

[196] Available in the ESMA "Advice on ICO and Crypto-assets" of 2019, pages 14-17. Among them, cybersecurity risks, hacks, and fraud.

[197] Unless crypto assets qualify as MiFID financial instruments or electronic money, they are likely to fall outside of the existing EU financial, potentially harming consumers and investors.

States recognize inconsistencies in the application of rules, with the consequent development of an uneven playing field, as well as the lack of ad hoc rules to address DLT-specific risks.[198]

3.3.1. A Fragmented Panorama

Most of existing applicable European financial law comes in the form of a Directive. As it is well-known, directives do not strike the objective of providing full harmonization since their transposition into national law may differ from jurisdiction to jurisdiction. Some Member States in fact implement Directives in a stricter way, whereas some others meet the demanded objectives in a more lenient way.

As suggested by the Survey[199] results, NCAs agreed upon the fact that no single rule can address all categories of crypto assets, however, some[200] jurisdictions implemented the directives in such a way that more[201] crypto assets are captured in the national financial legislation as compared to their peers.

Besides differences in EU law transposition, the legal uncertainty together with the concerns in relation to consumer protection, financial stability and market integrity brought some Jurisdictions to evaluate to impose themselves a bespoke regime for uncovered assets and their providers.

On the one hand, this would entail major supervision and safety within Member States, but as emphasized by ESMA, this would also imply that a level playing field at the EU level would not be reached, raising issues when considering the cross-border nature of crypto assets.

[198] See paragraph 83 of the ESMA Advice (footnote 196).
[199] Ibid.
[200] Among which, Italy.
[201] NCAs may have domestic categories of financial/investment products that are broader in scope with respect to the list of MiFID financial instruments, for example, addressing assets that are deemed to have an investment purpose or expectation of returns.

3.3.2. National Initiatives

Provided that no harmonized rule is in place at the international and regional level, a number of single jurisdictions decided to step up the pace from a legal perspective proposing their own regulatory framework, pushed by the need on the one hand to outline a token categorization and, on the other hand, to enhance consumer protection.

The advent of Blockchain applications in the financial sector spurred different kinds of reactions around the world. Few countries decided to play a pioneering role, proposing themselves as crypto-friendly jurisdictions, whereas others rejected the upcoming market, banning and prohibiting crypto exchanges. Some other countries instead proposed intermediate approaches, providing their own attempt at regulating crypto assets and their providers. Three Jurisdictions' initiatives, the Maltese, French and Italian one, will be proposed as follows.

3.3.3. Malta

Malta was the first European Member State to propose a favorable environment for crypto assets and their providers. In fact, back in 2013, the Malta Financial Service Authority introduced the possibility, for institutional investors, to invest in a fund providing access to crypto assets.

Malta, also named "the Blockchain Island"[202] after its firstcomer initiatives, started regulating blockchain, cryptocurrencies, and DLTs in 2018. Three law pieces[203] were enacted and were meant, first of all, to establish[204] a dedicated authority, the *Malta Digital Innovation Authority* (MDIA) whose role is to support innovation in financial technology.

In fact, the MDIA is responsible for the certification and supervision of *voluntary applications* of innovative technology service providers, with the aim of strengthening

[202] Read H. Sanchez "Malta Determined To Become the Blockchain Island: Regulations, Adoption, Binance Headquarters", Cointelegraph, April 2018, and Ganado Advocates "Snapshot Summary Of Three Bills Related to Blockchain Technology", June 2018.
[203] *MDIA, ITAS, VFAA.*
[204] Malta Digital Innovation Authority Bill.

the cooperation with other national competent authorities to boost technology, innovation, and the development of a well-established innovation hub in Malta.

Secondly, a setting on the certification of technology service providers was provided with the "Innovative Technology Arrangements and Service Bill" (ITAS Bill), which instead lays down the conditions to be satisfied by providers to obtain a certification for the provision of technology-related services.

Lastly, virtual assets service providers as well as the offering of virtual financial assets (ICOs) were regulated by the "Virtual Financial Assets Act Bill" (VFAA Bill), which consists in a bespoke regime for such assets at a national level. For instance, any ICO issuer or service provider must appoint an Agent,[205] the Virtual Financial Assets Agent, who makes sure the requirements are in place.

As far as the token classification is concerned, the VFAA Bill introduced a *test*, the "Financial Instrument Test", for the identification and classification of tokens – whose outcome would then allow determined types of platforms to have it traded.

The assets can be thus classified as "Virtual Token" (which corresponds to the Utility Token) or "Virtual Financial Asset" (namely MiFID Financial Instrument), or "E-Money" (EMD) with the aim of understanding whether the token should be covered by MiFID and related EU legislation, local legislation or none.

If the asset is classified as a Virtual Token,[206] then it falls outside the scope of financial regulation, whereas when it is framed as a Financial Instrument it would be covered by EU financial law, namely by the MiFID. Instead, where the token is deemed to be a Virtual Financial Instrument, under the definition "any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of

[205] In fact, the text of the VFA Act, Part IV, states that "application for a license under this Act shall be made solely through a VFA agent which is duly registered in terms of this Act in the form and manner required by the competent authority". The characteristics of the agent are defined in Chapter 590 of the Maltese Virtual Financial Assets Act, page 6.

[206] In order for the Test to determine whether a DLT asset is a Virtual Token, the asset may not be convertible into another DLT asset, it is exchangeable only within the DLT platform, it has no utility, value or application outside of the DLT platform.

value and that is neither (a) electronic money; nor (b) a financial instrument; nor (c) a virtual token", then, it would be ruled by the Virtual Financial Asset Act.

This last bill imposes authorization[207] requirements, which should be maintained on an ongoing basis for all ICO issuers and for all exchanges (VFA exchanges[208]) performing any of the services[209] present in the Act Second Schedule.[210] Examples of the services are in fact "operation of a VFA exchange and the placing of virtual financial assets".

This regime introduces a higher degree of investor protection, for example by imposing minimum disclosure requirements as well as the establishment of compensation schemes or arrangements and regulating the marketing of virtual financial assets.[211]

3.3.4. France

France adopted a supportive[212] regime for crypto assets and related service providers. In fact, for example, back in 2017, during the ICO boom, the French financial markets authority, the Autorité des marchés financiers (AMF), started a research program with the aim to get closer and cooperate with entrepreneurs of the digital finance panorama and ICO issuers. The program was named *UNICORN*, (Universal Node to ICO Research and Network) and aimed at offering project initiators a framework that would help them develop their projects in a safer manner, while ensuring customer protection. This dialogue would in fact provide the AMF with insights from the field which can be used

[207] Authorisation can be requested directly from the MFSA website.
[208] Chapter 590 of the Virtual Financial Asset Act defines VFA exchanges as follows: "VFA exchange means a DLT exchange operating in or from within Malta, on which only virtual financial assets may be transacted in accordance with the rules of the platform or facility, which is licensed by the competent authority under this Act to provide such services".
[209] VFA services, instead are defined as: "VFA service means any service falling within the Second Schedule when provided in relation to a DLT asset which has been determined to be a virtual financial asset", ibid.
[210] See Virtual Financial Asset Act, Chapter 590, Second Schedule, page 58.
[211] See again Ganado Advocates "Snapshot Summary Of Three Bills Related to Blockchain Technology", June 2018 and MFSA Virtual Financial Assets webpage.
[212] Interest in the cryptocurrencies and token field is proved by the French authorities as both the financial markets authority (AMF) and the banking authority (ACPR) have a Fintech Department that studies and analyzes innovation in banking and finance.

to understand possible implications for the traditional financial markets and the economy in general.[213]

Part of the current regulatory regime revolves around the "Plan d'action pour la croissance et la transformation des entreprises", also known as *PACTE law*, implemented in May 2019. It introduced a bespoke regime for digital assets service providers and initial coin offerings, which was then incorporated into the French Financial services act (Code monétaire et financier).

As far as the French regulatory framework is concerned, digital assets may be classified into three categories:

- *Utility tokens*, which represent a right on the issuer to access services or technologies – and are defined as those intangible assets that digitally represent one or more rights that enable the owner of the asset to access a service or a technology.
- *Cryptocurrencies*, which group the tokens used as means of exchange which do not necessarily represent a right on the issuer. They correspond to the so-called payment tokens.
- *Security tokens* corresponding to the MiFID definition of financial instrument, of course falling under the European Financial Services Law.

Instead, as for E-money, the AMF declared the definition of electronic money and that of digital asset is mutually exclusive, as digital assets do not represent monetary value.

Differently form Malta, the French regime does not present a compulsory registration for the provision of all services related to digital assets.

Instead, the French authority proposes a subset of activities for which registration is mandatory, and another subset of activities for which an opt-in regime is foreseen.

[213] See AMF news releases "The AMF publishes a discussion paper on Initial Coin Offerings and initiates its UNICORN programme", October 2017. The ICO discipline in France in comparison with other jurisdictions is also described in F. Annunziata paper "Speak, if you can: an alternative approach to the qualification of tokens and Initial Coin Offerings", page 30.

The French authority provides a list of activities for which a provider is considered a PSAN, namely a *Prestataire de Services sur Actifs Numériques*.[214]

The registration is mandatory[215] for the PSAN willing to provide the following activities[216] in France:

- "digital asset custody; and/or
- buying or selling digital assets in a currency that is legal tender; and/or
- trading of digital assets against other digital assets; and/or
- operation of a trading platform for digital assets".

For those activities the AMF is responsible for the assessment of the reputation of managers as well as of the organization's beneficial owners, and seeks clearance from the ACPR (Autorité de Contrôle Prudentiel et de Résolution). The registered Digital Service Asset Provider must comply with all the obligations to contrast money laundering and terrorist financing.

For the remaining activities, registration is not mandatory; however, where PSANs provide one or more services belonging to the general list,[217] they may decide to be licensed[218] by the AMF upon request. Of course, for the license to be granted, PSANs must comply with prudential and conduct requirements on an ongoing basis. Those licensed will be then recognized and published in the AMF website.[219] It should be noted that, however, where PSANs are not willing to obtain the license, they are free to continue to operate anyway.

[214] Available in the Financial monetary code, article L. 54-10-2.
[215] Without which, services cannot be provided.
[216] Available in the AMF website, Obtaining a DASP registration/optional licensing.
[217] See footnote 214.
[218] The AMF Questions & Answers on the DASP Regime provides a clarification as regards the licensing opportunity: "In addition to registering, applicants may also ask the AMF for a license pursuant to Article L. 54-10-5 of the Monetary and Financial Code for the same services and for other digital asset services, if applicable. They will therefore be subject to the provisions of Articles L. 54-10-5 and D. 54-10-6 of the said code and to the relevant provisions of Title II of Book VII of the AMF General Regulation".
[219] Having positive reputational consequences. See footnote 216.

3.3.5. Italy

The third approach to be treated is the Italian one.

As previously underlined, no ad hoc rules apply to exchanges directly, but only as a consequence of the appraisal of the legal nature of crypto assets.[220] In fact, European Jurisdictions commit themselves to a case-by-case analysis to understand whether digital assets may classify as MiFID Financial instruments, and eventually apply all the requirements foreseen by the Directive.

In detail, existing MIFID II rules relating to investment services, operation of trading venues, and financial products public offerings have been transposed in Italy in the Financial Consolidated Act[221] (FCA).

For the purposes of the application of the Italian regulatory framework, four subcategories of crypto assets were identified:

- *Utility-type*, which provides some utility function other than that of a means of payment or exchange for external goods or services;
- *Payment-type*, which can be assimilated to cryptocurrencies;
- *Security-type*, which would fall in the category of Financial Instruments;
- *Financial products*, a further category that can be considered Italian-branded.

Utility-type tokens are not regulated as far as the Italian legislation is concerned, whereas Payment-type tokens may fall under the definition of E-money.[222] Conversely, it is interesting to analyze how *Security-type* crypto assets and *Financial Products* are treated in relation to the Italian Financial Consolidated Act.

As explained in the MiFID paragraph and transposed in the Italia Legislation, the *provision of services and activities* that are listed in the Italian FCA *Annex I, section A* "Sezione A - Attività e servizi di investimento" in relation to any of the Financial

[220] As previously explained, the applicability of the existing legal framework to platforms trading and exchanging crypto assets in secondary markets is linked to the legal qualification of the tokens.
[221] See the Italian Financial Consolidated Act "Testo Unico Finanziario (TUF)".
[222] As previously explained.

Instruments present in Annex I, Section C "Sezione C - Strumenti finanziari",[223] if performed professionally and for the Public, then it would constitute a reserved activity, for which authorization is required.

In fact, if crypto assets are classified as Financial Instruments, the platform in which they are traded and exchanged would then be considered a MiFID trading venue,[224] such as Regulated Market, Multilateral trading facility, or Organized trading facility.

However, where the token is not classified as Financial Instrument nor as E-money, it may not be necessarily excluded from the application of Italian law. Interestingly, Italy adopted a *broader approach* than the one proposed by the MiFID, introducing another purely domestic category of assets: while many crypto assets that present features which are investment-like[225] are not subject to securities and financial market law in most jurisdictions, the Italian law includes the category of "Financial Product" too.

Article 1, paragraph 1, letter (u) of the Italian FCA defines financial products (*prodotti finanziari*) as follows:

"Per prodotti finanziari s'intendono gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria; non costituiscono prodotti finanziari i depositi bancari o postali non rappresentati da strumenti finanziari".[226]

The Financial Products category is broader[227] in scope than that of Financial Instruments, being comprehensive of *Financial Instruments and any other form of investment of financial nature*.

[223] Which reflects the one provided in the MIFID II, ANNEX I Sections A and C. Security tokens can be assimilated to transferable securities or other types of MiFID financial instruments as discussed in the previous paragraphs; as for the Italian FCA, transferable securities correspond to "Valori mobiliari", which are defined by *art. 1 bis* of the TUF.
[224] Following a bottom-up approach.
[225] Not security-like.
[226] That is, financial products are defined as financial instruments and *any other form* of investment of financial nature, from which deposits not represented by financial instruments are excluded.
[227] And in fact, it embeds Financial Instruments, among others.

The Italian Authority CONSOB provided[228] further details on the definition of financial products, determining three main features that might suggest an asset could fall under this domestic category.[229] They are:

- the investment of capital;
- the promise/expectation of a financial return derived from the capital invested;
- the assumption of a financial risk directly connected and related to the investment of capital.

Further distinctive elements that distinguish an investment whose nature is merely financial are the prevalence of financial aspects over the material ones and the promise of a return (in form of an increase in the value of the capital invested, different from an appreciation of the asset over time) at the moment of the establishment of the contractual relationship.[230]

The financial products category may be suitable for the inclusion of hybrid tokens, which are difficult to classify and regulate in the vast majority of jurisdictions, as they may have remarkable financial content and are often placed to retail investors[231] via public offerings.

However, the provision of services in relation to crypto assets that qualify as financial products does not imply licensing obligations, as in that case the provider of services and activities in relation to such assets would not be defined as an investment firm, being financial products excluded from the "Strumenti Finanziari" list.

---

[228] See CONSOB Discussion Paper "Le offerte iniziali e gli scambi di cripto-attività. Documento per la Discussione" (March 2019), page 5.

[229] And in particular in relation to the "residual" component of "investments of a financial nature"

[230] On the other hand, according to the CONSOB, the scope of *financial product* does not cover investments in consumer products, namely transactions involving the purchase of goods or services designed to procure the investor the enjoyment of the asset that may satisfy non-financial needs. However, the distinction between a financial product and a consumer good may require a complex analysis: in this regard, a financial product may be characterized by the existence of a secondary market and the way the product is marketed. This debate is still wide open, in particular in relation to the Metaverse.

[231] It should be remarked that where a token that may be classified as a financial product is offered to retail investors, which are considered by the MiFID and TUF the type of client requiring the highest protection, then they would be assimilated to financial instruments and would require the preparation of a Prospectus as well.

However, this does not mean such activities are totally exempted from regulation,[232] as the Italian financial law states that the promotion of investment products performed by means of distance communication[233] (i.e., when the parties are not simultaneously and physically in the same place, so, for example, through an exchange platform[234]) is reserved to providers of services and activities that are already authorized to perform some types of investment services. Examples include the management of trading platforms of such assets, provided that the *promotion of financial products* takes place, and that it *takes place through distance communication techniques*.

The accent in this particular case is thus posed on the *methods* through which the activity takes place, according to which rules on the distance promotion and placement of financial products and rules on public offerings may apply.[235]

For example, if an exchange platform advertises an asset emphasizing and promising a financial return arising from the investment of capital on that asset through the platform, then, the distance promotion of a financial product may take place.[236]

Once again, a meticulous case-by-case analysis should be carried out in order to identify a financial product's characteristics (or the existence of a financial instrument) and understand whether, for example, remote marketing and prospectus rules apply.

3.4. The Italian Case: OAM Register

In the first semester of 2022, Italy introduced mandatory registration in a register for Virtual Assets Service Providers for anti-money laundering purposes. In February 2022, the Decree of the Italian Ministry of Economics and Finance dated January 13, 2022, was published in the Official Journal.[237] The decree regulates the time frame and the ways in

[232] See A. Minto, "The Legal Characterization of Crypto-Exchange Platforms", Global Jurist 2021, page 10.
[233] *Art. 32* of the TUF.
[234] Which is performed online.
[235] See again, A. Minto "The Legal Characterization of Crypto-Exchange Platforms", pages 10, 11, 12.
[236] CONSOB banned in fact some websites offering crypto-currencies trading services, for which a financial return was advertised and promised. Ibid.
[237] See Gazzetta Ufficiale n.40 dated 17 February 2022, page 3.

which virtual assets service providers must communicate they operate within the Italian territory.[238]

In particular, VASPs should apply for registration in a special section of the *Organismo Agenti e Mediatori*[239] (OAM) Register. The section is constructed so as to broaden the scope of application, which was limited to fiat currency[240] exchanges.

The Decree identified and defined two types of service providers: providers of services in relation to virtual currencies ("prestatori di servizi relativi all'utilizzo di valuta virtuale") and wallet providers ("prestatori di servizi di portafoglio digitale"), which are defined, respectively, as:

- "Any natural or legal person providing services related to the use, transfer, and preservation of virtual currency as well as the exchange of virtual currencies for currencies that are legal tender including their digital representation or for other virtual currencies. Other services such as the issuance, offering transfer compensation, and any other service that is instrumental for the acquisition, negotiation, and intermediation as regards of its exchange, are included. The above-mentioned services shall be performed as a business[241] and can be performed online too;[242]

[238] See Decreto del Ministero dell'economia e delle finanze 13 gennaio 2022 on "modalità e tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria operatività sul territorio nazionale, nonché le forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia, ai sensi dell'articolo 17-bis, comma 8-ter, del D. lgs. 13 agosto 2010, n. 141 e successive modificazioni", Gazzetta Ufficiale n. 40.

[239] OAM is responsible for the management of the registers reporting information on entities engaging in financial services and activities: "organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi, ai sensi dell'art. 128 -undecies del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385".

[240] Intended as legal tender.

[241] Professionally.

[242] Article 1, comma 2 (b) of the Decree "prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o soggetto diverso da persona fisica che fornisce a terzi, a titolo professionale, anche on-line, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute";

- Any person being involved in the safekeeping of private cryptographical keys on behalf of their clients with the aim of holding, storing, and transferring virtual currencies professionally and also online".[243]

In this regard, the decree also provides the definition of *virtual currency*,[244] which is intended as the digital representation of value that is not issued nor guaranteed by a central bank or a public authority, which is not necessarily attached to a legal tender, and which is used as a medium of exchange for buying goods or services or for investment purposes, and which is stored and traded electronically.

It can be noticed that the decree has some similarities with the Italian anti-money laundering and counter-terrorist financing decree[245] and in fact, both the above-mentioned definitions and requested information were taken by the Italian Regulator from *Decree 231/2007*.

Definitions appear to be broad in their scope, particularly those regarding the category of service providers in relation to virtual currencies. For this reason and with the aim of pointing out the services and activities the providers of which should apply for registration, the decree also presents a more detailed list[246] in Annex II:

1. "Services that are instrumental to the use and exchange of virtual currencies and/or their conversion into fiat currencies or their digital representation, including those convertible into other virtual currencies;
2. Issuance and offer of virtual currencies;
3. Transfer or compensation in virtual currencies;

[243] Article 1, comma 2 (c) of the Decree "prestatori di servizi di portafoglio digitale: ogni persona fisica o soggetto diverso da persona fisica che fornisce, a terzi, a titolo professionale, anche on-line, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali";
[244] Article 1, comma 2 (f) of the decree: "valuta virtuale: la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente".
[245] Decreto Legislativo 21 novembre 2007, n. 231 on anti-money laundering and counter-terrorism financing.
[246] The ministerial Decree provides a detailed description, which comes in the form of a list, of services to which registration requirements provided by Decree 141/2010 apply.

4. Any other service that is instrumental to the acquisition, negotiation and/or intermediation for the exchange of virtual currencies (e.g. execution, reception, transmission of data in relation to virtual currencies on behalf of third parties as well as the placement and advice in relation to virtual currencies).
5. Digital Wallet Services".[247]

It is then specified that the mere emission of virtual currency, which is not offered nor marketed to the public, does not constitute a service for which registration In the OAM Special Section is required.

The list of services is provided by the Ministry for the purpose of informing which Virtual Asset Service Providers are required to communicate[248] the OAM they perform a business activity related to virtual currency within the Italian territory.

In fact, when communicating the exercise of a business activity in relation to virtual currencies, the provider must state which kind of services and activities it performs or is willing to perform, among other information.

Notwithstanding the presence of the list, which should clarify the scope of the decree, it is noticeable how some services and activities description remains quite broad. In fact, the wording and the terminology often do not precisely indicate a determined service and activity, leaving space for interpretation. For example, the first service, namely "Services that are instrumental to the use and exchange of virtual currencies and/or their conversion into fiat currencies or their digital representation, including those

[247] The Decree describes them as follows: "1. Servizi funzionali all'utilizzo e allo scambio di valute virtuali e/o alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali; 2. Servizi di emissione, offerta di valute virtuali; 3. Servizi trasferimento e compensazione in valute virtuali; 4. Ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio di valute virtuali (es. esecuzione, ricezione, trasmissione di ordini relativi a valute virtuali per conto di terze parti, servizi di collocamento di valute virtuali, servizi di consulenza su valute virtuali); 5. Servizi di portafoglio digitale"; Allegato 2 (Annex 2) of the Decree, page 7. The Decree adds that the mere emission of virtual currencies which is not performed to the public as a business does not require a subscription to the special section of the OAM register.

[248] As can be noticed by the wording of Article 3 "Comunicazione dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale" (page 4) and "l'indicazione della tipologia di servizio prestato tra quelli elencati nell'allegato 2 del presente decreto, che ne costituisce parte integrante" (page 5), both for physical and legal persons.

convertible into other virtual currencies"[249] does not make clear the meaning of "services that are instrumental to the use and exchange", as no precise examples are provided to the reader.

The same can be seen in the fourth service, which is similar to the first one as it starts with the wording "Any other service", which again, rises doubts regarding the type of services the regulator is willing to include.[250]

Moreover, the accent is posed to the way in which services are performed, which should be professionally (as a business and in a continued manner), and to the public.[251]

Some other issues can be displayed.

First, it is not clear how regulated intermediaries (for example banks or investment firms) should behave if they decide to perform the activities listed in Annex II of the Decree: it is unclear whether they should apply for registration or not, raising concerns in relation to the scope of application of the decree as well as the lack of proper coordination with other existing regulations.[252]

Second, the Decree applies within the Italian territory, "L'esercizio sul territorio della Repubblica italiana […]"[253] raising cross-border issues and boosting fragmentation among Member States.

Third, although the Decree imposes registration[254] and not licensing,[255] if the provider does not communicate the provision of one or more of the above-mentioned services within the time frame determined in article 3 of the Decree, they would be considered illicit.

[249]See Annex II, page 7: Servizi funzionali all'utilizzo e allo scambio di valute virtuali e/o alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali".
[250] See Annex II, page 7. For example, it is not understood whether advisory services are included, as they embed per se a broad category of services.
[251] Although a definition of public is not provided.
[252] For instance, there may be an overlap with the Anti-money laundering decree.
[253] See article 3 comma 1.
[254] For which certain requirements should hold
[255] For which discretion is left to authorities for the authorization to perform a reserved activity

Fourth, the Decree, whose consultation started four years prior to its publication, presents some features which make it unsuitable, for example following the fact that providers are treated as money changers, which should have a physical place where the currency exchange service takes place.[256]

As mentioned above, in order to complete the registration[257] in the register, some requirements should be satisfied.

Such requirements are the same as those foreseen for those performing currency exchange services.[258] In the first place, providers operating within the Italian territory, also online, should establish a legal residence[259] within the Italian territory if they do not have one, including those operating in Italy and having their domicile outside[260] the Italian territory.

All requirements foreseen by *article 17-bis, comma 2* of Decree 2010/141[261] shall be met by all above-mentioned providers in order to successfully register in the special section of the OAM Register. Additionally, such requirements should be met also when the performance of the services in relation to virtual currencies takes place *online only*.

The Decree specifies that registration is compulsory for:

- Those willing to operate within the Italian territory;
- Those already offering such services within the Italian territory.

In particular, those already offering services in relation to virtual currencies or digital wallets should complete the registration within 60 days from the availability date of the special section of the Register.[262] Newcomers should instead register before the business is started, and the OAM verifies the requirements are met.

[256] As Virtual Currencies cannot be exchanged physically.
[257] As precised in the Decree, the mere communication of the performance of one or more services present in the Decree does not consist in the registration.
[258] See Article 17- bis, comma 2 of the legislative decree 2010/141.
[259] Through a physical place/office.
[260] Both Member States and Third-countries actors.
[261] See footnote 258.
[262] Which corresponds to the time frame of 90 days from the date the Decree is enacted.

The registration imposes also some ongoing obligations on the providers, which shall transmit the OAM the data reported in Article 5 of the Decree with the data specified in Annex I[263] on a quarterly basis. Such data are the same required by the anti-money laundering directive and consist of client information and data on the operations conducted by single clients, both in relation to fiat currencies and to virtual currencies.[264]

Of course, that would not be simple for foreign providers operating in the Italian territory, as they would then be required to extract data relative to their Italian clients, hence perform additional computer science-related analysis. Moreover, those subject to OAM registration and ongoing requirements are also subject to AML requirements, which may sometimes overlap.

Once registered, where ongoing requirements are not met,[265] the OAM can suspend the registration for a period between three months and one year, and can also withdraw the registration where requirements are no longer met, quarterly communications are repeatedly violated, in case of inactivity,[266] or where the services are no longer provided upon termination of the activity.

[263] Information to be transmitted to the Authority (from Annex I of the Decree) are the following: "Informazioni da trasmettere all'OAM ai sensi dell'Art. 5, comma 1a. Dati identificativi del cliente come di seguito specificati: 1. cognome e nome; 2. luogo e data di nascita; 3. residenza; 4. codice fiscale/partita IVA, ove assegnato; 5. estremi del documento di identificazione. B. Dati relativi all'operatività complessiva per singolo cliente (1), come di seguito specificati: 1. Controvalore in euro (2), alla data dell'ultimo giorno del trimestre di riferimento, del saldo totale delle valute legali e delle valute virtuali riferibili a ciascun cliente; (3) 2. Numero e controvalore complessivo in euro, alla data dell'ultimo giorno del trimestre di riferimento, delle operazioni di conversione da valuta legale a virtuale e da virtuale a legale riferibili a ciascun cliente; 3. Numero delle operazioni di conversione tra valute virtuali riferibili a ciascun cliente; 4. Numero delle operazioni di trasferimento di valuta virtuale in uscita e in ingresso da/verso il prestatore di servizi relativi all'utilizzo di valuta virtuale riferibili a ciascun cliente; 5. Numero e controvalore in euro, alla data dell'ultimo giorno del trimestre di riferimento, dell'ammontare delle operazioni di trasferimento di valuta legale in uscita e in ingresso da/verso il prestatore di servizi relativi all'utilizzo di valuta virtuale, riferibili a ciascun cliente e suddivise per trasferimenti in contante e strumenti tracciabili".

[264] The OAM holds the data for a period of 10 years, ensuring they are safely stored and can be easily recovered if necessary. Such transmission requirement represents a meeting point with the traditional banking and financial system in general, as also banks and investment firms are required to communicate aggregate data in relation to their clients' operations.

[265] In relation to quarterly communications of client's information.

[266] For more than one year, unless reasonable reasons are provided.

Where registration is not completed within the periods provided by the Decree, the provider is punished for abusive exercise with an administrative penalty.[267]

[267] Which amounts to a pecuniary sanction from €2.065 to €10.329; it should be noted that the penalty is not so high if compared to the annual fee requested to the registered providers, which amounts to € 8.300 plus an additional annual fee.

Chapter IV: The Upcoming Regulatory Framework

With the following, the upcoming Regulatory Framework in relation to crypto exchanges will be presented.

In particular, the Chapter dives into the Digital Finance Package, with a focus on the Markets in Crypto Assets Regulation, whose Title V will be then compared to the Italian Decree D.lgs. 13 Gennaio 2022[268] on the special section of the OAM Register, and will touch on the upcoming Anti-Money Laundering Package.

4.1. The Digital Finance Package

The Digital Finance Package has its roots in the FinTech Action Plan,[269] which was designed to push the use of rapid advances in new technologies, such as blockchain, artificial intelligence, and cloud services in the financial sector.

"The future of finance is digital. We saw during the lockdown how people were able to get access to financial services thanks to digital technologies such as online banking and fintech solutions. Technology has much more to offer consumers and businesses and we should embrace the digital transformation proactively, while mitigating any potential risks. That's what today's package aims to do. An innovative digital single market for finance will benefit Europeans and will be key to Europe's economic recovery by offering better financial products for consumers and opening up new funding channels for companies." [270]

These were the words of Vice President Valdis Dombrovskis in relation to the adoption by the European Commission of the *Digital Finance Package*, highlighting the usefulness

[268] See footnote 238.

[269] Fintech Action Plan: summary available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_1403.

[270] "Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses". Speech by Valdis Dombrovskis, Press release, Brussels, September 2020.

of a common strategy for Europe, which would boost Europe's competitiveness and innovation in the financial sector, while ensuring financial stability.

The package aims at supporting the digital finance potential while mitigating the risks, in order to build a future-ready economy for consumers and enterprises.

The Digital Finance Package is composed of a Digital Finance Strategy, a Retail Payments Strategy, the Markets in Crypto Assets Regulation proposal, a Regulation on a Pilot Regime for Market Infrastructures and a proposal for a European regulatory framework on digital operational resilience.

4.1.1. The Digital Finance Strategy

The Digital Finance Strategy poses itself four high-level objectives:[271]

- The creation of a Digital Single Market for financial services;[272]
- The drafting of a regulatory framework that facilitates innovation;
- The mitigation of the risks posed by the digital transformation;[273]
- The creation of a European financial data space with the aim of promoting data-driven innovation.[274]

The benefits include, among others, the increase of the financial market integration in the Banking Union and the Capital Markets Union thanks to a well-functioning cross-border digital finance, the availability of better financial products for consumers, and of new opportunities for businesses (especially small and medium enterprises) to access funding, to ease Europe's economic recovery and finally to strengthen Europe's autonomy in financial services.

[271] Commission "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU" COM (2020) 591 final.
[272] Enabling European consumers to access cross-border services and helping European financial firms to scale up their businesses across borders.
[273] Safeguarding financial stability and consumer protection, market integrity, fair competition, and security.
[274] Including enhanced access to data and data sharing within the financial sector.

Such benefits can be achieved through the creation of EU-wide interoperable digital identities in finance, the promotion of open finance,[275] the development and application of a comprehensive EU regulatory framework for crypto assets, the development of a set of common rules on digital operational resilience, which would effectively mitigate the risks arising from the digital transformation and finally by ensuring "same activity, same risks, same rules" principle applies.

4.1.2. The Digital Operational Resilience Act

The European Commission highlighted in the 2018 Fintech Action Plan the importance of enhancing the level of digital operational resilience to ensure its technological safety and good functioning, in order to enable the smooth functioning of financial services across Europe.

In order to pursue the above-mentioned objectives, the European Commission laid down a Legislative proposal for a European regulatory framework on digital operational resilience, with the aim of preventing and mitigating cyber threats.[276]

In particular, the Digital Operational Resilience Act tackles *information communication technologies risks*, which are now common to the financial sector too, especially due to the increasing dependency of financial firms on software and digital processes.[277]

[275] Through the creation of a network for data sharing for the EU financial sector and beyond.
[276] European Commission "Proposal for a Regulation of the European Parliament and of 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 final.
[277] Ibid, Recital 2, page 12. "Digitalization covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, insurance underwriting, claim management and back-office operations. Finance has not only become largely digital throughout the whole sector, but digitalization has also deepened interconnections and dependencies within the financial sector and with third-party infrastructure and service providers".

What can be underlined is that the Commission does so through a Regulation, providing the maximum level of harmonization in this context with the aim of increasing security to a never-reached-before level.[278]

In fact, the European Systemic Risk Board (ESRB) underlined[279] that the high level of interconnectedness characterizing financial entities, markets, and financial market infrastructures, together with the interdependency of their ICT system, may pose threats to financial stability which can be systemic. This is due to the fact that localized cyber incidents have the potential to spread from one entity to the whole financial system, irrespectively of geographical boundaries, causing adverse consequences for the stability of the European financial system.

To this aim, the selected option[280] was to introduce a financial services digital operational resilience act (concretized with the DORA Proposal) that would enable a European framework that addresses regulated financial entities and introduces a framework for the supervision of critical ICT third-party providers. This option would benefit consumers and investors too, as this framework would reduce ICT incidents both in number and magnitude, as well as boost trust in the financial services industry.

With this Act, the Commission seeks to ensure all firms are able to withstand ICT-related threats, both in the traditional sector and in the fintech one, and to impose strict standards on them so as to reduce disruption impacts.

[278] The proposal text suggests that although after the Great Financial Crisis measures were taken in order to govern financial risks, digital operational resilience was only addressed in a limited manner, and as a consequence indirectly promoted national initiatives and consequently fragmentation. The European Commission was pushed to elaborate on this risk also by the 2019 ESAs Joint technical advice (Joint Advice of the European Supervisory Authorities To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector) that suggested a more coherent approach in addressing ICT risk in finance was necessary, the European Commission on its Fintech Action Plan (FinTech Action plan: For a more competitive and innovative European financial sector) as well as from ongoing international initiatives such as from the Basel Committee on Banking Supervision's Cyber-resilience: Range of practices, and Principles for sound management of operational risk.

[279] In its 2020 Report on *Systemic cyber risk*.

[280] Conveyed by the majority of Stakeholders. See page 6 of the Proposal.

4.1.3. Retail Payments Strategy

The Retail Payment Strategy[281] aims at providing safe, fast and reliable payment services to European citizens and businesses, seeking to create a fully integrated retail payments system as well as instant cross-border payment solutions.

The Retail Payment Strategy poses itself with the aim of reducing the risks derived from market fragmentation, setting out a clear direction, and elaborating a single, coherent and overarching policy framework.

To this aim, the Strategy focuses on the promotion of "digital and instant payment solutions with pan-European reach, of innovative and competitive retail payments markets, on the creation of efficient and interoperable retail payment systems and other support infrastructures and of efficient international payments, including remittances".[282]

4.1.4. Pilot Regime for Market Infrastructures based on Distributed Ledger Technology

Instead, the Pilot Regime for Market Infrastructures based on DLT aimed at developing a protected environment for firms and ensuring an innovation-friendly legal approach.

While designing the Digital Finance Package, the European Commission differentiated two broad categories of crypto assets: those already regulated by existing European Financial Legislation, namely crypto assets that classify as *financial instruments*, and those falling outside the scope of existing legislation.

[281] Commission "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU" COM (2020) 592 final.
[282] Ibid.

As regards the former category of crypto assets, a pilot regime for market infrastructures willing[283] to trade and settle financial instruments in crypto asset form was introduced and published in the European Official Journal in June 2022.[284]

The roots of this initiative, and of the Package in general, lie in the European Commission FinTech Action Plan when, back in 2018, the Commission asked the EBA and the ESMA to assess to what extent the existing EU financial regulatory framework was suitable to regulate crypto assets. The two of them responded with an Advice,[285] in which they affirmed that whilst some crypto assets may fall under the scope of existing legislation,[286] most crypto assets are unregulated,[287] leaving consumers and investors exposed to the related risks.[288] Additionally, the advice reported that "provisions in existing EU legislation may inhibit the use of DLT".

This is, inter alia, one of the reasons why the Pilot Regime for DLT-based market infrastructures was created: in fact, the regime was designed in order to give both market agents and regulators and supervisors the opportunity to gain experience right in the field of the possible benefits and threats this innovative technology offers, as well as to let them understand how to operate within the law.[289]

In fact, the regime revolves around a *sandbox approach*, an approach whose ultimate goal is to help actors to develop a secondary market for crypto assets, and in general, the adoption of DLT in the trading and post-trading phases.

This approach is constructed so as to let firms perform their activities in a protected environment, where they are exempted from the financial market regulatory framework for a period of time: this would in fact give firms operating with DLT the time to

[283] This should enable market participants and regulators to gain experience with the use of DLTs exchanges.
[284] Commission "Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU".
[285] See EBA "Report with advice for the European Commission on crypto-assets" (January 2019) and ESMA "Advice on Initial Coin Offerings and Crypto-Assets" (January 2019).
[286] Although the correct application is not straightforward.
[287] Except for AML purposes.
[288] See *ESAs Warnings* to consumers on the risks posed by crypto assets.
[289] See A. Minto, F. Annunziata, "Il nuovo Regolamento UE in materia di Distributed Ledger Technology - Analisi del nuovo DLT Pilot Regime" (July 2022), Non solo diritto bancario.

understand how to properly adapt to the rules that traditionally apply to investment firms.[290]

However, the scope of the Regulation is very specific, since it only applies to financial instruments[291] issued on the DLT, namely what is commonly referred to as tokenized financial instruments issued on a distributed ledger technology.

Tokenized financial instruments can be in fact defined as the "digital representation of financial instruments on distributed ledgers or the issuance of traditional asset classes in tokenized form to enable them to be issued, stored and transferred on a distributed ledger".[292]

For the purpose of the sandbox and in particular for exemptions, three types of DLT market infrastructures[293] were identified:

- DLT Multilateral trading facilities (DLT MTF);[294]
- DLT settlement systems (DLT SS);[295]
- DLT trading and settlement systems (DLT TSS).[296]

[290] In this regard, the Regulation on a Pilot Regime for DLT-based market infrastructures reports the following: "Union financial services legislation was not designed with distributed ledger technology and crypto-assets in mind, and contains provisions that potentially preclude or limit the use of distributed ledger technology in the issuance, trading and settlement of crypto-assets that qualify as financial instruments. Currently, there is also a lack of authorised financial market infrastructures which use distributed ledger technology to provide trading or settlement services, or a combination of such services, for crypto-assets that qualify as financial instruments. The development of a secondary market for such crypto-assets could bring multiple benefits, such as enhanced efficiency, transparency and competition in relation to trading and settlement activities".

[291] However, some limitations to financial instruments admitted to trading or recorded on DLT market infrastructure exist, and they are listed in article 3 of the Regulation (they relate, for example, to market capitalization, issue size, market value).

[292] See Paragraph 3 of Regulation EU 2022/858.

[293] Ibid, see recital 12.

[294] Defined in article 2 as "a multilateral trading facility that only admits to trading DLT financial instruments".

[295] Defined in article 2 as "a settlement system that settles transactions in DLT financial instruments against payment or against delivery, irrespective of whether that settlement system has been designated and notified in accordance with Directive 98/26/EC, and that allows the initial recording of DLT financial instruments or allows the provision of safekeeping services in relation to DLT financial instruments".

[296] Defined in article 2 as "a DLT MTF or DLT SS that combines services performed by a DLT MTF and a DLT SS".

The three of them, however, are required to accomplish MiFID II and CSDR[297] requirements.

Further requirements and exemptions allowed vary upon the type of facility, and are described respectively in Articles 4, 5, and 6[298] of the Regulation. Specific authorization can be requested by licensed[299] investment firms in order to perform a DLT MTF, a DLT SS, or a DLT TSS in compliance with Articles 8, 9, and 10[300] of the Regulation and should point out the exemptions demanded.

The authorization is limited to a time period of six years and should be granted by National Competent Authorities, which are in turn required to forward a copy of the request to the European Securities and Markets Authority.

This Regulation, along with the one for a bespoke regime for crypto assets, the MiCAR, represents a big step in order to provide adequate levels of consumer protection, increase the legal certainty regarding crypto assets, and ease businesses to adopt blockchain, distributed ledger technology, and crypto assets, while ensuring financial stability.

4.2. Market in Crypto Assets Regulation

Instead, for those assets not covered by existing financial regulation, an ad hoc piece of law was drafted in order to capture their specificities and grant harmonization at the European Union level.

[297] Commission "Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories".
[298] Respectively reporting "Requirements and exemptions regarding DLT MTFs", "Requirements and exemptions regarding DLT SSs", and "Requirements and exemptions regarding DLT TSSs".
[299] MiFID II or CSDR.
[300] Respectively reporting "Specific permission to operate DLT MTF", "Specific permission to operate DLT SS", and "Specific permission to operate DLT TSS".

The piece of law is the Market in Crypto Asset Regulation,[301] for which an agreement was reached[302] at the end of June 2022. It was born with the aim of filling in the gaps in the European Financial Regulation and coordinating the different pieces of law in the sector, also supporting the creation of a Digital Single Market and the Capital Markets Union.

This piece of law comes in the form of a Regulation too, establishing a harmonized framework imposing requirements for issuers of crypto assets and crypto asset service providers wishing to operate in the European Union, and will be directly applicable in all Member States, leaving no room for regulatory arbitrage caused by differences in the transposition into national law, as opposed to the majority of the legislations applicable to the FinTech industry.[303]

While drafting the MiCAR, several approaches were considered: among them, an opt-in regime and a full harmonization regime. The choice went to the latter, provided that it could ensure the creation of a pan-European market for crypto assets, hence representing a high-level achievement for service providers. While the first regime could be less burdensome for small issuers and service providers that could decide not to opt-in, the second one would ensure a higher level of legal certainty, providing major investor protection, market integrity, and financial stability and reducing market fragmentation across Member States.

In fact, the lack of a uniform framework and difficulties in the interpretation of rules prevented service providers from scaling up their activity at the European level. Moreover, the proliferation of national initiatives forced them to familiarize themselves with different legislations and obtain multiple authorizations or registrations, with the obligation to comply on an ongoing basis with divergent national laws. This came with high costs and increased legal complexity, which represented a huge barrier to entry and

[301] Commission "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937" COM (2020) 593 final.
[302] In this regard, see the European Union Council Press Release "Digital finance: agreement reached on European crypto-assets regulation (MiCA)" June 2022.
[303] Largely composed of directives that, for their very nature, leave room for discretion, as formerly reported in relation to the MiFID transposition in Member States' law.

operate within the crypto asset business, limiting the development of related activities at the Union level. Such divergences are responsible for the creation of an uneven playing field for crypto asset service providers and hinder the functioning of the internal market.

The MiCAR was born in order to provide a common framework aiming at overcoming the fragmentation across Member states and reducing the complexity and costs for firms operating in this space. Additionally, it would enable actors to reap the benefits of the internal market, providing legal certainty, promoting market integrity, and providing consumers and investors with appropriate levels of protection.

To this aim, the proposal, which covers, among others, stablecoins and e-money tokens, presents four high-level objectives:

- *Legal certainty*: the previous chapter highlighted how national initiatives and doubts about the interpretation of existing laws were detrimental to consumer protection, market integrity, and financial stability purposes. In order to let a crypto asset market develop and grow within the European Union, a clear and sound legal framework is necessary in order to define the regulatory treatment of all crypto assets.
- *Support innovation*: the development of the European crypto asset market, together with the larger adoption of DLT, is determined by the extent to which the framework adopted is supportive of innovation purposes.
- *Ensure appropriate levels of consumer and investor protection and market integrity*: as formerly discussed, crypto assets that are not covered by existing regulations leave consumers and investors unprotected from risks, which should be addressed to limit their negative consequences.
- *Ensure financial stability*: the evolution of crypto assets may pose risks to financial stability, especially when it comes to those potentially having a larger application (i.e., stablecoins). Therefore, safeguards should be imposed on such assets in order to address potential risks to financial stability in a timely manner.

4.2.1. The structure

The proposed Regulation is intended to regulate crypto assets that do not fall under the scope of current existing law (e.g., *stablecoins*), imposing strict requirements for issuers in Europe, as well as safeguards on Crypto Asset Service Providers through the registration for the provision of services.

In order to fulfill the aforementioned objectives, the MiCAR is structured as follows.

Title I includes the subject matter, the scope of the Regulation, and useful definitions. It underlines that the Regulation applies to crypto assets service providers and issuers, which will then be mentioned and regulated in the subsequent titles. Importantly, Article 2 of the Proposal highlights that the Regulation is limited in scope to crypto assets that *do not qualify* as financial instruments, deposits, or structured deposits under EU financial services legislation.[304]

Title II rules the offerings and marketing to the public of crypto assets other than asset-referenced tokens and e-money tokens, setting out general duties when it comes to offerings of crypto assets to the public and specifying when the drafting of a white paper is necessary.[305] Interestingly enough, with this Title the regulator *makes a common market practice mandatory*: in general, the vast majority of market players used to publish an informative paper containing information regarding the asset offered, similarly to a prospectus. This highlights the influence of financial markets legislation.

Title III is divided into six chapters and extensively regulates the issuers of asset-referenced tokens, with particular attention to conduct requirements, prudential requirements, rules on conflicts of interest and reserve assets,[306] as well as the obligation to have a wind-down procedure in place.

[304] Also in the MiCAR the Commission makes use of delegated acts to the ESAs, requiring them to draft technical standards to better capture specificities and developments.
[305] See Article 5,7,8 of the Proposal on the White Paper. See Article 4 for exemptions in relation to the drafting of the White Paper.
[306] The very feature of ART requires more precise regulation: in particular, some rules about the underlying apply, for example, concerning the composition and maintenance as well as stabilization.

Similarly to Title III, Title IV deals with E-money Tokens, describing requirements from the authorization of issuers to prudential safeguards and as regards the drafting of the white paper.

Title V, which is of major interest for the sake of this Thesis, deals with the provisions on authorization and operating conditions of Crypto Asset Service Providers, and will be better addressed in the following paragraph.

Title VI sets out prohibitions and requirements to avert market abuse in relation to crypto assets.

Title VII lays down the powers and competencies of the various authorities, among which the National Competent Authorities, the EBA, and the ESMA. It also deals with administrative sanctions and penalties and any other measures to be taken in case of a breach. Supervisory powers in relation to issuers of significant e-money tokens and asset-referenced tokens are also set out, together with those in relation to the most relevant crypto asset trading platforms, custodians and credit institutions providing services in relation to the significant asset referenced token.

Title VIII discusses the exercise of delegated acts from the Commission to the ESAs.

Title IX reports the transitional and final provisions, including the obligation for the Commission to produce a report evaluating the impact of the Regulation.

What can be noted from the mere description of the Titles is that the Proposal somehow mirrors the MiFID and other existing European Financial Markets Laws, capitalizing on the experience in financial services regulation and transferring the approach to crypto assets. This can be seen, for example, when addressing transparency and disclosure in relation to issuance, operation, organization, and governance of crypto asset service providers, consumer protection and market abuse, but also in the distinction between significant and non-significant providers, which is commonly referred to in banking law.

4.2.2. Title V

Providers of services in relation to crypto assets, called Crypto Asset Service Providers (CASPs) under the Regulation, find a tailored regulatory framework in Title V on

"Authorisation and operating conditions for Crypto-Asset Service providers". The title, which is composed of four chapters, designs the authorization requirements and procedure, as well as the operating conditions for providers.

Chapter 1,[307] titled "Authorisation of crypto-asset service providers", sets out the provisions on authorization, including the information applicants shall provide when drafting the request, how the application is assessed, and the reasons for which authorization can be denied or withdrawn.

Article 53 deals with the authorization of CASPs and reports 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".

From the above recital, the legislator does make clear that the services provided by CASPs are considered *reserved activities* by law, and as for the banking and financial services, it is underlined that conditions for authorization should be met on an ongoing basis.

When providing the authorization, competent authorities shall declare the provision of services for which each CASP is authorized, and when a CASP is willing to perform other services for which it is not licensed, it shall request the competent authority an *extension* of its authorization.

Moreover, *Article 53* allows Providers to passport their services to the other Member States, allowing them to fully reap the benefits of the Single Market. It can be understood from the wording "An authorisation as a crypto-asset service provider shall be valid for the entire Union and shall allow crypto-asset service providers to provide throughout the Union the services for which they have been authorised, either through the right of establishment, including through a branch, or through the freedom to provide services."[308]

[307] Covering Articles 53-58.
[308] See Article 53, recital 3 of the Proposal.

Article 54 lays down the information that shall be contained in the *application module*; information regards, but is not limited to, governance arrangements, complaints handling procedures, a description of the procedure for the segregation of the client's crypto assets and funds, and the description of the service(s) provided by the CASP.[309]

Article 55 deals with the "Assessment of the application for authorisation and grant or refusal of authorization". The Article states that authorization should be granted or denied by competent authorities within three months from the date of receipt of a complete application. Interestingly, the article adds emphasis to the *level of discretion* authorities may have, which can be understood from the sentence "Competent authorities […] shall adopt a fully reasoned decision granting or refusing an authorisation as a crypto-asset service provider. That assessment shall take into account the nature, scale and complexity of the crypto-asset services that the applicant crypto-asset service provider intends to provide."[310]

Once authorization is approved or denied, the competent authorities shall inform the ESMA about their decision, which in turn would add authorized CASPs to a register reserved for CASPs,[311] which is established and kept by the ESMA.

On the other hand, *Article 56* regulates *authorization withdrawal*. Reasons behind withdrawal may be, but are not limited to, the infringement of the Regulation, the lack of subsistence of authorization conditions, the involvement in money laundering and/or terrorist financing by the entity, or simply the lack of performance of the service for which it was previously authorized for a period longer than 18 months. Information in relation to the withdrawal of the authorization shall be laid down by the ESMA in the CASPs Register.

Article 57 imposes the establishment of the above-mentioned Register of authorized crypto asset service providers, which is controlled by the ESMA.

[309] Among which crypto assets custody, the running of a trading platform, exchange (fiat-for-crypto or crypto-to-crypto), execution of orders, and transmission of orders.
[310] See Article 55, recital 5 of the Proposal.
[311] See Article 57 of the Proposal.

Among the information, ESMA shall point out in the register "the list of crypto-asset services for which the crypto-asset service provider is authorized,[312] any other services provided by the crypto-asset service provider not covered by this Regulation with a reference to the relevant Union or national law,[313] any withdrawal of an authorisation of a crypto-asset service provider."[314]

When a Crypto Asset Service Provider is willing to provide the services for which it is authorized in a cross-border fashion, namely in more than one Member State, the competent authority shall be duly informed in compliance with *Article 58*, which discusses the "Cross-border provision of crypto-asset services".

Information to be provided to the competent authority consists of, for example, the list of Member States in which the CASP is willing to operate.

Article 58 then sets out information and details on the *operation* of CASPs involved in cross-border activities, and in particular on the responsibilities of the *Home* and *Host* Member States Competent Authorities.

Chapter 2,[315] titled "Obligation for all crypto-asset service providers" imposes various requirements on CASPs.

In particular, Article 59 imposes the obligation to "act honestly, fairly, and professionally in accordance with the best interests of their clients and prospective clients as well as the obligations to provide their clients with fair, clear and not misleading information, warn clients of risks associated with purchasing crypto-assets and make their pricing policies publicly available on their websites".[316]

Articles 60 and 61 impose, respectively, prudential and organizational requirements.

[312] See Article 57 (d) of the Proposal.
[313] See Article 57 (f) of the Proposal.
[314] For a period of five years. In this regard, see Article 57.
[315] From Article 59 to Article 65.
[316] See Article 59 of the Proposal, Recitals 1 to 4.

Prudential requirements shall be in place on an ongoing basis and can take the form of own funds[317] or an insurance policy covering the Member States in which the CASP performs its services. In the case in which the form of an insurance policy is selected, the policy shall include the elements listed in paragraph 5 of the Article, among which eventual losses arising from business disruption or system failures and, where applicable, gross negligence in the safeguarding of clients' crypto assets and funds.[318]

Organisational requirements are instead related to the management body, system, and procedures in place. The management body of the CASP shall possess the characteristics of being of good repute and competent, in terms of qualifications, experience, and skills to perform their duties,[319] as required by the Banking Law and Financial Markets Law.

As set out in paragraph 6, "Crypto-asset service providers shall take all reasonable steps to ensure continuity and regularity in the performance of their crypto-asset services. To that end, crypto-asset service providers shall employ appropriate and proportionate resources and procedures, including resilient and secure ICT systems" and where ICT systems and procedures are interrupted, "the preservation of essential data and functions and the maintenance of crypto-asset services, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of crypto-asset services" shall be granted.

Duly attention is posed to the systems and procedures in this Article, being the themes of security, integrity, and confidentiality of information crucial in this field.

Article 62 instead requires CASPs to provide the competent authority with all the relevant information in case the management body is subject to changes.

Importantly, *Article 63* lays down rules in relation to the *safekeeping of the client's funds*: paragraph 1 states that "Crypto-asset service providers that hold crypto-assets belonging to clients or the means of access to such crypto-assets shall make adequate

[317] Of Common Equity Tier 1 (CET1) as provided by Articles 25 and 26 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions.
[318] See points (e) and (f) of Article 60. Of course, it deals with providers also offering custody and safekeeping services.
[319] See Article 61, paragraph 1.

arrangements 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".

Moreover, CASPs possessing clients' funds shall place them with a central bank or a credit institution, which in turn should be accurately separated from the bank's funds and from other clients' funds.

Article 64 imposes on CASPs the obligation to introduce an effective complaint handling procedure, which should be transparent and free of charge. It underlines that, when receiving a complaint, CASPs shall investigate it in a timely manner and provide the client with information on its findings and the outcome of the investigation.

Conflicts of interest are regulated in *Article 65*,[320] and are treated in a similar way as for investment firms in MiFID II.[321] In general, "Crypto-asset service providers shall maintain and operate an effective policy to prevent, identify, manage and disclose conflicts of interest",[322] and where conflicts of interest are inevitable, they should inform their clients through their website.[323]

The last Article of this Chapter, namely *Article 66*, deals with "Outsourcing"; it requires CASPs that rely on third parties for the provision of operational functions to take all actions in order to minimize operational risk. CASPs in this case shall, inter alia, make sure the relationship between them and their clients is not affected, and that outsourcing does not represent a condition for which authorization requirements may be altered.

Chapter 3[324] designs *service-specific requirements* for each class of *CASPs,* to which a dedicated Article is foreseen. Article 3, paragraph 9 of the MiCAR proposes seven classes

[320] On the "Prevention, identification, management and disclosure of conflicts of interest*".*
[321] See Article 23 of MiFID II.
[322] See Article 65, paragraph 1 of the Proposal.
[323] See Article 65, paragraph 2 of the Proposal. The Article captures the nature of the business, which takes place mainly online.
[324] From Article 67 to Article 73.

of services, which are identified and addressed according to their very features in a specific manner.

They are:

- "Custody and administration of crypto-assets on behalf of third parties";
- "Operation of a trading platform for crypto-assets";
- "Exchange of crypto-assets against fiat currency or exchange of crypto-assets against other crypto-assets";
- "Execution of orders for crypto-assets on behalf of third parties";
- "Placing of crypto-assets";
- "Reception and transmission of orders on behalf of third parties";
- "Advice on crypto-assets".

Article 67 deals with "Custody and administration of crypto-assets on behalf of third parties", which is defined as "safekeeping or controlling, on behalf of third parties, crypto-assets or the means of access to such crypto-assets, where applicable in the form of private cryptographic keys".[325]

A CASP offering custody and administration services of crypto assets on behalf of its clients shall enter an *agreement* with them, specifying the distribution of duties and responsibilities. A *register of positions* shall be kept by the CASP, which shall update it with all transactions performed by its clients in a timely manner. Moreover, a *custody policy* shall be in place to ensure the safekeeping of crypto assets and/or clients' cryptographic keys. This obligation is particularly relevant since it protects clients from the possibility that the CASP loses the clients' crypto assets, or the rights related to those assets due to frauds, cyber threats, or negligence.

The Article also requires the CASP to *inform its clients of their position* at least quarterly through a statement of position and to contact them where operations to be undertaken require approval.

[325] See Article 3 of the Proposal, paragraph 10.

Additionally, the Article requires the CASP to *duly segregate* its own holdings from those belonging to the clients, making sure they are attributed to different addresses on the DLT.

Importantly, CASPs "shall be liable to their clients for loss of crypto-assets as a resulting from a malfunction or hacks up to the market value of the crypto-assets lost".[326]

Article 68 deals with the "Operation of a trading platform for crypto-assets", defined as "managing one or more trading platforms for crypto-assets, within which multiple third-party buying and selling interests for crypto-assets can interact in a manner that results in a contract, either by exchanging one crypto-asset for another or a crypto-asset for fiat currency that is legal tender".[327]

First, CASPs authorized for the provision of this service are required to lay down in a transparent manner the operating rules for the trading platform by setting the requirements, due diligence, and approval processes previously to the admission[328] of crypto assets to the trading platform, the fee structure and the criteria for the participation in the trading activities.

Moreover, CASPs *shall not admit* to trading those crypto assets presenting an *inbuilt anonymization function*, unless the authorized service providers are able to track their holders and their transaction history; additionally, CASPs are not authorized to deal on their own account.

CASPs operating a trading platform shall have in place effective systems and procedures to ensure they provide resilient, correct, and safe trading systems, and shall provide their clients with bids and asks in relation to the crypto assets available in their platform on a continuous basis, as well as real-time price, volume, and time of the transactions.

Article 69 lays down specific requirements for the "Exchange of crypto-assets against fiat currency or exchange of crypto-assets against other crypto-assets". They are defined, respectively, as "concluding purchase or sale contracts concerning crypto-assets with third parties against fiat currency that is legal tender by using proprietary

[326] See Article 67, Paragraph 8, which is of great importance for client protection purposes.
[327] See Article 3, paragraph 11 of the Proposal.
[328] Which can only be introduced where a white paper is released, unless exempted by article 4.

capital" and "concluding purchase or sale contracts concerning crypto-assets with third parties against other crypto-assets by using proprietary capital".[329]

Such CASPs shall indicate the type of clients they accept and disclose it through the establishment of a non-discriminatory commercial policy.

According to the Article, they shall release crypto assets prices, or the method used for determining it, and they are required to execute orders on behalf of their clients at the prices displayed at the moment the order was received. Therefore, they shall disclose orders and transaction details.

Article 70 governs the "Execution of orders for crypto-assets on behalf of third parties". This activity is described as "concluding agreements to buy or to sell one or more crypto-assets or to subscribe for one or more crypto-assets on behalf of third parties".[330]

When performing the above-mentioned service, CASPs shall commit to granting the client the *best possible result* in terms of execution[331] unless the provider executes the order following specific instructions provided by the client. To this aim, they shall put in place an order execution policy that results in the prompt, fair, and swift execution of clients' orders and shall make it available to their clients, including any related change.

The "Placing of crypto-assets" is regulated by *Article 71*. It consists of "the marketing of newly-issued crypto-assets or of crypto-assets that are already issued but that are not admitted to trading on a trading platform for crypto-assets, to specified purchasers and which does not involve an offer to the public or an offer to existing holders of the issuer's crypto-assets".[332]

CASPs authorized for this service shall enter a contract with the issuer of crypto assets, before which they shall make clear the type of placement, the transaction fees and the timing of the operation. Information in relation to the targeted purchasers and conflicts of interest shall be ruled out in accordance with *Article 65*.[333]

[329] See Article 3, paragraphs 12 and 13 of the Proposal.
[330] Ibid, paragraph 14.
[331] Considering, for example, price, costs, and speed.
[332] See Article 3, paragraph 15 of the Proposal.
[333] In particular, where CASPs place the crypto asset with their clients and where the price is unfair (e.i., overestimated or underestimated).

Article 72 sets out the requirements concerning the "Reception and transmission of orders on behalf of third parties", which is defined as "the reception from a person of an order to buy or to sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution".[334]

Authorized providers are required to implement an effective procedure for the timely transmission of orders for their execution on a trading platform for crypto assets or to another CASP. In order to perform such service, CASPs shall not receive any benefit, remuneration, or discount and prevent the improper use of the information in relation to the client's pending orders.

Lastly, *Article 73* treats the "Advice on crypto-assets", which is defined in Article 3, paragraph 17 as "offering, giving or agreeing to give personalised or specific recommendations to a third party, either at the third party's request or on the initiative of the crypto-asset service provider providing the advice, concerning the acquisition or the sale of one or more crypto-assets, or the use of crypto-asset services".

In particular, an *assessment* of the client's knowledge and experience as far as crypto assets are concerned, as well as the client's objectives and financial situation (including the ability to bear losses) should be performed in order to measure the compatibility of crypto assets with the client.

Of course, the CASP shall make sure the assessment is performed on all clients and that the information collected is reliable and updated at least every two years.

Advisors should possess extensive knowledge and experience in order to recommend crypto assets to the client only when in their interest. They should also present and make sure they understand the risks involved in purchasing crypto assets and shall warn clients that the value of crypto assets may fluctuate.

Advisors should provide their clients with a report summarizing the advice given in a durable medium and shall contain the client's demands and needs as well as the advice provided.

[334] See Article 3, paragraph 16 of the Proposal.

The *fourth*[335] and last chapter of Title V discusses the rules on the acquisition of crypto assets service providers.

Article 74 is in fact about the "Assessment of intended acquisitions of crypto-asset service providers".

It disposes of rules on qualified holdings and the notification to competent authorities, which should approve or deny the acquisition.[336]

Article 75 continues on the purpose of Article 74 and discusses the "Content of the assessment of intended acquisitions of crypto-asset service providers".

More precisely it indicates the elements competent authorities should assess for the acquisition purpose, for example, the reputation of the management body as well as their experience, and whether the acquired CASP continues to successfully comply with the requirements set out in the Title.

4.2.3. MiCAR: Positive Aspects and Critiques

The MiCAR is however embedded with some limitations.

Many experts[337] from the field claimed that the Regulation, whose Proposal was laid down back in 2020 and which is going to enter in force in 2024, will be outdated by that time. This is due to the fact that digital finance and in particular the crypto sector are evolving at a pace at which the regulator is not keeping up, leaving some aspects unregulated.

This is the reason for which ECB President Christine Lagarde called for a "MiCAR II" and defined the current Proposal as "MiCAR I" during the hearing of the Committee on Economic and Monetary Affairs.[338]

---

[335] See Articles 74 and 75.

[336] See Article 74 for more precise information.

[337] Among which, Andrea Pantaleo. See F. Luini "MiCA: il rischio di un regolamento nato Vecchio", FUNDSPEOPLE (July 2022).
Some improvements are also suggested in the paper "The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy" of November 2020 by Dirk A. Zetzsche, F. Annunziata, Douglas W. Arner, and Ross P. Buckley.

[338] During the hearing of the committee on Economic and Monetary Affairs of 20 June 2022

Christine Lagarde, who shared the view of the ESRB, claimed in fact that what would be actually needed is a Regulation that is able to capture:

- The risk in relation to *interconnectedness*, regulating the exposure of financial institutions to crypto assets;
- *Staking* and *lending*, which are now getting popular;
- *Decentralized Finance*, which is controversial when regulating intermediaries, as they may not be identifiable.[339]

Additionally, a critique was moved to the MiCAR structure and content, claiming that the regulator tried to apply to a fast-changing, peculiar and innovative sector, rules that are typical of traditional financial entities, noting that the Proposal resembles the MiFID in many aspects.

As regards the content, it is claimed that the Markets in Crypto Assets Regulation focuses too much[340] on stablecoins, which, on the one hand, might be reasonable assuming their potential application for the future, but on the other hand, left some loopholes in relation to, for example, DeFi and NFTs,[341] which are becoming more and more important as far as recent market developments are concerned.

Moreover, experts pointed out that while the European Union promoted the Package as a set of innovation-friendly rules that would enhance the safety of the market, the output might not let small firms develop their services because of a too stringent regulatory framework, leaving the business in the hands of institutional investors only.

Lastly, during a Conference[342] on the MiCAR, experts debated about the fact that the Digital Finance Package is, as its name suggests, a package on digital finance, whereas

[339] In fact, the MiCAR identifies the subjects that fall under the Regulation, which are clearly identifiable entities such as issuers and providers, for example, which are not comprehensive of subjects operating in decentralized finance.
[340] Valeria Portale, "La proposta MiCAR: sfida normativa per lo sviluppo del mercato Crypto", Novembre 2021, Sole 24 Ore Finanza.
[341] As regards NFTs, the Proposal in fact covers only the fractions of NFTs as they wouldn't present the feature of being unique and thus not interchangeable, but instead, fractions would be interchangeable among themselves.
[342] "Il Regolamento Market in Crypto Asset – Discussione Pubblica sul futuro della regolamentazione Europea MiCA". Discussion panel with Stefano Capaccioli, Massimiliano Nicotra, Andrea Pantaleo, Claudia Morelli, Tamara Belardi, Martina Granatiero, Marco Tullio Giordano, Sara Noggler e Davide Zanichelli.

the MiCAR is supposed to be applied to assets different from financial instruments, highlighting that crypto assets that are declared to be non-financial assets are then treated as if they were financial assets, and the same requirements that are in place for financial actors are applied to CASPs too. This, once again, underlines the similarities between the MiCAR and the MiFID but also in relation to Banking Law.[343]

However, the Proposal presents plenty of benefits too.

First of all, it represents the first substantive law piece for Service Providers, thanks to which they will be subject to prior authorization from a National Competent Authority before starting their activities, and consequently adhere to a number of requirements in order to continue to operate: this will increase their credibility as they will be supervised to the same extent as traditional financial institutions.

Additionally, consumer protection, which is one of the main concerns of the ESAs and the European Authorities in general, is extensively treated, both in relation to CASPs,[344] and in relation to Asset Reference Tokens and E-Money Tokens.[345]

Most importantly, the MiCA comes in the form of a Regulation, providing a harmonized legal framework at the European Union level. It will wipe out the legal uncertainty that was creating issues both for end-users and service providers, which had to adapt to many national initiatives that, in turn, were preventing them from scaling up their businesses. This will instead be possible when MiCA comes into force, reducing costs for Service Providers and boosting the efficiency of the European Single Market.

Moreover, a positive consideration should be made as regards the relationship between the MiCAR and AML/CFT. In fact, the previous version of the Proposal contained in its subject matter an additional point that conferred upon the MiCAR the prevention of money laundering and terrorist financing. This created doubts and confusion and, above all, contrasted one of the major scopes of the Regulation, which aimed at coordinating

[343] This can be noted, for instance, in the categorization of institutions into more and less significant as provided in the SSM Regulation. In fact, issuers of significant asset-referenced tokens will be supervised by the European Banking Authority.

[344] As can be seen, for example, in the requirement to create a compliant handling procedure which is now lacking in the current market practice.

[345] This is seen, for example, in the obligation to provide a whitepaper with the necessary information to make a reasoned decision and in relation to marketing communications.

existing rules and filling in the gaps in the European financial law. Fortunately, as reported in the Press Release on the MiCA, "to avoid any overlaps with updated legislation on anti-money laundering (AML), which will now also cover crypto-assets, MiCA does not duplicate the anti-money laundering provisions".[346]

4.3. Title V versus OAM Register: a comparison

As described in Chapter 3, back in February 2022, the Ministry of Economics and Finance Decree dated 13 of January 2022 was published in the Italian Official Journal[347] with the aim of imposing the registration of VASPs into a special section of the OAM Register for anti-money laundering purposes.

It is worth comparing the fifth Title of the MiCAR with the Decree, although they differ in purpose. In fact, as formerly pointed out, the MiCAR major aim is that of, on the one hand regulating crypto assets not covered by existing financial regulation while, on the other, of being the substantive law piece for crypto assets service providers that was missing, imposing, among others, prudential, organizational and conduct requirements, as well as service-specific requirements.

Differently, the registration requirement to the OAM Register special section imposes the providers of services in relation to cryptocurrencies and wallet providers the obligation of the subsequent transmission of data in relation to their clients' operations for anti-money laundering and counter-terrorist financing purposes on a quarterly basis.

First, the two pieces of law differ in the types of requirements they impose: on the one hand, the OAM imposes a *compulsory registration*, for which it is sufficient to meet predetermined requirements; on the other hand, the MiCAR imposes *mandatory authorization to operate* as CASPs, which is subject to some levels of discretion by authorities, which "shall adopt a fully reasoned decision granting or refusing an authorisation as a crypto-asset service provider".[348]

[346] See European Council Press Release "Digital finance: agreement reached on European crypto-assets regulation (MiCA)" July 2022.
[347] See the Italian Official Journal (number 40, page 3).
[348] See MiCAR Proposal, Title V, Article 55, paragraph 5.

Secondly, it should be noticed that the Decree Text is composed of eight articles and two annexes, whereas the fifth Title of the MiCAR counts twenty-one articles, which exclusively deal with CASPs.

Moreover, it stands out that the services referred to in Title V, Chapter 3 are duly defined in Article 3 of the Regulation "Definitions", and the formerly mentioned chapter provides ad-hoc, detailed requirements for each type of service. It cannot be said the same for the Decree definition of providers of services in relation to crypto assets, which is the following:

"Any natural or legal person providing services related to the use, transfer, and preservation of virtual currency as well as the exchange of virtual currencies for currencies that are legal tender including their digital representation or for other virtual currencies. Other services such as the issuance, offering transfer compensation and any other service that is instrumental for the acquisition, negotiation and intermediation as regards its exchange are included. The above-mentioned services shall be performed as a business[349] and can be performed online too".[350] The services are then specified in Annex II as follows:

- "Services that are instrumental to the use and exchange of virtual currencies and/or their conversion into fiat currencies or their digital representation, included those convertible into other virtual currencies.
- Issuance and offer of virtual currencies;
- Transfer or compensation in virtual currencies;
- Any other service that is instrumental to the acquisition, negotiation and/or intermediation for the exchange of virtual currencies (e.g., execution, reception, transmission of data in relation to virtual currencies on behalf of third parties, as well as the placement and advice in relation to virtual currencies).

[349] Namely professionally.

[350] See Article 1, comma 2 (b) "prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o soggetto diverso da persona fisica che fornisce a terzi, a titolo professionale, anche on-line, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute".

- Digital Wallet Services".[351]

The list, whose aim was to make the services to which the registration obligation is compulsory, ended up being too broad and confusing for Providers, especially compared to[352] MiCAR definitions, which are outlined as follows in Article 3 of the Regulation:

- "Crypto-asset service provider means any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis";
- "crypto-asset service means any of the services and activities listed below relating to any crypto-asset:

  (a) the custody and administration of crypto-assets on behalf of third parties;

  (b) the operation of a trading platform for crypto-assets;

  (c) the exchange of crypto-assets for fiat currency that is legal tender;

  (d) the exchange of crypto-assets for other crypto-assets;

  (e) the execution of orders for crypto-assets on behalf of third parties;

  (f) placing of crypto-assets;

  (g) the reception and transmission of orders for crypto-assets on behalf of third parties

  (h) providing advice on crypto-assets";
- "the custody and administration of crypto-assets on behalf of third parties means safekeeping or controlling, on behalf of third parties, crypto-assets or the means of access to such crypto-assets, where applicable in the form of private cryptographic keys";
- "the operation of a trading platform for crypto-assets means managing one or more trading platforms for crypto-assets, within which multiple third-party buying and selling interests for crypto-assets can interact in a manner that results

[351] See Annex II of the Decree.
[352] For example, the MiCAR provides a clear definition of the provision of advice on crypto assets, which is instead not provided in the Decree.

in a contract, either by exchanging one crypto-asset for another or a crypto-asset for fiat currency that is legal tender";

- "the exchange of crypto-assets for fiat currency means concluding purchase or sale contracts concerning crypto-assets with third parties against fiat currency that is legal tender by using proprietary capital";
- "the exchange of crypto-assets for other crypto-assets means concluding purchase or sale contracts concerning crypto-assets with third parties against other crypto-assets by using proprietary capital";
- "the execution of orders for crypto-assets on behalf of third parties means concluding agreements to buy or to sell one or more crypto-assets or to subscribe for one or more crypto-assets on behalf of third parties";
- "placing of crypto-assets means the marketing of newly-issued crypto-assets or of crypto-assets that are already issued but that are not admitted to trading on a trading platform for crypto-assets, to specified purchasers and which does not involve an offer to the public or an offer to existing holders of the issuer's crypto-assets";
- "the reception and transmission of orders for crypto-assets on behalf of third parties means the reception from a person of an order to buy or to sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution";
- "providing advice on crypto-assets means offering, giving or agreeing to give personalised or specific recommendations to a third party, either at the third party's request or on the initiative of the crypto-asset service provider providing the advice, concerning the acquisition or the sale of one or more crypto-assets, or the use of crypto-asset services".[353]

This reveals to be confusing for Providers, who should ask themselves whether they are providing a service for which the OAM Registration is mandatory, and introducing further costs and thus, barriers to entry.

[353] See Article 3 of the Proposal, Definitions 8 to 17.

As for the Decree, the aim was clearly to make the applicability as broad as possible in order to capture eventual changes in the provision of services or the addition of new ones.

Finally, the OAM Register registration requirement also raises some doubts in relation to the upcoming European AML Package, as some requirements, in particular in relation to the transmission of data to the Authority, may overlap, making the register requirements burdensome for Providers.

4.4. The Upcoming AML/CFT Package

In July 2021, the European Commission presented a grand package composed of a proposal for a Regulation and a Directive to boost the Anti-money laundering and counter-terrorist financing regulatory framework for the European Union.

The Package aims at improving the recognition of suspicious transactions and activities, and successfully preventing criminals from using the financial system to launder the proceeds of illicit activities.

The Package consists of four pieces:

- The creation of a new, tailored European anti-money laundering Authority, namely the Anti-Money Laundering Authority (AMLA);[354]
- A new Regulation on anti-money laundering and counter-terrorist financing;[355]
- The sixth Directive on anti-money laundering and counter-terrorist financing;[356]

[354] See Commission "Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010" COM (2021) 421 final.
[355] See Commission "Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing" COM (2021) 420 final.
[356] See Commission "Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849" COM (2021) 423 final.

- The revision of the Transfer of Funds Regulation.[357]

With the above-mentioned measures, an eye is kept in particular on technological innovation such as virtual currencies, the global nature of terrorist organizations, and the increasingly integrated financial flow in the Single Market, helping obliged entities to be more compliant, especially in relation to cross-border activities.

First, with the creation of the new Anti-Money Laundering and Countering the Financing of Terrorism Authority, the AMLA, supervision as regards AML/CFT will be enhanced, and cooperation among Financial Intelligence Units and National Competent Authorities will be boosted.

In fact, the AMLA will be responsible for the coordination of the National Competent Authorities and ensure that rules are effectively applied in the member states. It will therefore establish a single, integrated system in relation to AML/CFT at the EU level, based on common supervisory methods; moreover, the AMLA will directly oversee the riskiest financial institutions in order to better address potential threats. It will coordinate NCAs and support the cooperation among FIUs for the detection of cross-border risks. It will be established in 2023 and will be fully operational by 2026.

Thus, the AMLA will:

- Introduce a central, integrated supervisory system for the European Union in relation to AML/CFT, providing a harmonized supervisory methodology;
- Directly supervise the riskiest entities to limit AML/CFT risk;
- Monitor and coordinate NCAs;
- Promote cooperation among financial intelligence units for the creation of a joint analysis which will be helpful in the detection of cross-border crimes.

The Package also foresees a Directive, namely the sixth AML/CFT Directive and a Regulation on AML/CFT.

The Directive, which will replace the fourth Directive on AML/CFT amended in 2018, will deal with all the specificities for which transposition in the national law is necessary,

[357] See Commission "Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets" COM (2021) 422 final.

such as in relation to areas that require a tailored approach in relation to the national-specific risks to money laundering; it also contains rules in relation to National Competent Authorities and Financial Intelligence Units responsibilities.[358]

Instead, a Regulation[359] was laid down in order to maximize harmonization at the European Union level, since delays in implementation and divergence in national rules are leading to an increasingly fragmented approach when dealing with Anti-Money Laundering and Countering the Financing of Terrorism. The new Regulation will provide directly applicable rules, providing a more detailed and granular regime to contrast money laundering and the financing of terrorism, while ensuring convergence among the Member States. In fact, a number of Regulatory Technical Standards will be included, for example as regards Customer Due Diligence, for which a specific and harmonized EU-wide approach is necessary.

Additionally, the list of obliged entities will be integrated:[360] as previously pointed out, the ESAs recommended reviewing and integrating the list of obliged entities, in particular in relation to VASPs. Interestingly, the AML Package would harmonize the definition of providers, as the list of obliged entities will include CASPs as defined in the MiCAR,[361] for example extending the application of AML/CFT safeguards to providers of

[358] As can be seen in the sixth directive proposal Subject Matter as follows: "This Directive lays down rules concerning:
(a) measures applicable to sectors exposed to money laundering and terrorist financing at national level;
(b) the identification of money laundering and terrorist financing risks at Union and Member States level;
(c) the set-up and access to beneficial ownership, bank account and real estate registers;
(d) the responsibilities and tasks of Financial Intelligence Units (FIUs);
(e) the responsibilities and tasks of bodies involved in the supervision of obliged entities,
(f) cooperation between competent authorities and cooperation with authorities covered by other Union acts".

[359] The Regulation lays down rules concerning the measures to be applied by obliged entities, transparency requirements on the beneficial ownership for legal entities, and arrangements and measures to limit the misuse of bearer instruments, as displayed in Article 1 of the Regulation Proposal.

[360] Service providers in relation to crypto assets will be integrated but also other entities will be then obliged to perform AML/CFT safeguards. They are, for example, Crowdfunding service providers falling outside the scope of the EU Crowdfunding Regulation, Mortgage credit intermediaries, and Consumer Credit providers different from financial institutions.

[361] In fact, the new proposal will integrate the services that are already included in the currently in force Directive with those pointed out in the MiCAR.

services with crypto assets only. The new standards set in the Package will thus provide a definition of crypto assets and crypto asset service providers which include a number of services and activities that corresponds to[362] and even goes beyond the FATF requirements.

The Regulation also rules out the possibility to open and use anonymous crypto assets accounts.

As for the recast of the 2015 Regulation on the Transfer of Funds, it will extend its scope to that of crypto assets, requiring CASPs to obtain major, or better, full information on the sender, as well as on the beneficiary involved in the transaction in crypto assets.[363]

They will be required to identify the parties involved in the transactions in relation to crypto assets and fiat currency for AML/CFT purposes:

- Where a traditional electronic transfer takes place;
- Where a transfer of crypto assets takes place between two obliged entities.[364]

Such rules will increase the extent to which CASPs are regulated and monitored, also ensuring compliance with the FATF Recommendations.[365]

It can be noticed that the Package contains three Regulations, providing for the first time a harmonized regulatory framework for the prevention of money laundering and terrorist financing, creating the single Anti-Money Laundering Rulebook.

[362] Aligning European legislation to the FATF Standards.
[363] Read Banca d'Italia "Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività", page 12.
[364] Even where one of them is not a CASP.
[365] For further information, see the European Commission Document reporting Q&A as regards the new Package "Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)".

Concluding Remarks

Although the debate is still going to continue, and although experts already called for MiCAR II, as of today the path to embrace new technologies and in particular crypto assets and their providers brought to important results from a Financial Law Perspective.

Regulators identified both the benefits and risks posed by this sector and tried to address them in the best possible manner, considering the speed at which it is evolving.

First, Regulators followed an "adaptative" approach in order to include part of crypto assets and service providers in the regulatory perimeter through the application of existing rules.

Later, Regulators started a process to tackle them directly, as the adaptative one revolved around the legal characterization of assets, which may differ from jurisdiction to jurisdiction, raising regulatory arbitrage and widespread legal uncertainty. It can be appreciated that the organizational, conduct, and prudential aspects of providers, as well as anti-money laundering and counter-terrorist financing provisions were drafted in the form of Regulations, reducing the fragmentation which was characterizing the European Union, and providing higher legal certainty and stronger consumer protection.

The political agreement on MiCA dated 30 June 2022 marks a landmark turning point in the approach to crypto assets, with a global, worldwide impact, making the European Union the first global multi-jurisdiction to have uniform rules on crypto assets, with the MiCAR posing itself as a real game-changer from a financial law perspective.

With this Package the European Union is getting ready to embrace innovation consistently with high standards of safety and resilience, and reducing operational costs, legal complexity, and legal uncertainty and thus boosting the scaling up of crypto asset activities in the Union. In fact, the Upcoming Regulatory framework poses the basis for the development of an integrated market for new technologies, favoring innovation in digital finance and attracting innovative businesses.

ANNEX I: Blockchain Forensics

Blockchain technology presents a number of risks and opportunities for which it finds applications in many sectors.

In fact, blockchain is already adopted by many industries, among which the automotive, healthcare, government, telecommunications, manufacturing, and of course, finance.[366]

However, blockchain applications also benefitted criminals, which, as mentioned in Chapter II, exploited it in order to commit illicit activities.

On the one hand, the blockchain allows full traceability of transactions, which are engraved in the blockchain and cannot be deleted,[367] and are freely[368] consultable by everyone. This feature of blockchain allows all data and transactions concerning a determined crypto asset to be reconstructed, making it better than paper-coin from an anti-money laundering perspective, as transactions in cash cannot be traced at all.

However, subjects performing the transactions are not easily distinguished and thus identified. It is acknowledged that the risk of money laundering is assessed through the identification of subjects, which lies, in fact, at the base of the customer due diligence procedure.

Difficulties in the identification of subjects are thus making it difficult for entities to correctly perform safeguards; however, in this regard, the upcoming AML Package will introduce the obligation to collect sufficient information for the identification of both subjects involved in transactions.

Currently, experts in the field developed some tools which, used in combination with AML "more traditional" safeguards, may be helpful for intermediaries to actually

[366] Additional industries are available in IBM website, "Blockchain for industries". Interestingly, Forbes provided a list of 15 industries which could benefit from blockchain applications in the article "15 Industries That Could Significantly Benefit From Blockchain Technology", June 2022, Expert Panel, Forbes Technology Council.
[367] Without leaving visible tracks.
[368] In public blockchains, which are used by criminals.

retrieve the necessary information for the identification of criminals using blockchain for their illicit activities.

Back in 2021, the Italian Financial Intelligence Unit published a communication[369] on the prevention of financial crime in the pandemic context in which it brought some examples of crimes, among which those performed with cryptocurrencies. In particular, it highlighted their frequent use for the purchase of drugs on the darknet and suggested a possible approach for the mitigation of risks.

In fact, the Italian FIU proposed the use of *blockchain forensics* in order to track activities for the purpose of detecting suspicious transactions.[370]

As mentioned in the previous chapters, the Financial Action Task Force elaborated[371] on further risk factors[372] concerning virtual assets and virtual asset service providers for Risk-Based-Approach purposes, which, however, can be assessed only through the use of blockchain forensic tools.

Blockchain forensics consists of tools[373] that exploit blockchain structural features (i.e., traceability) for the reconstruction of a single transaction's history.

Pseudo-anonymity of blockchains allows transactions to be associated with a wallet through a pseudonym, the public key, and gives access to a list of transactions marked by the so-called hash.[374] If transactions are visualized in a list, they do not convey any useful information for the recognition of suspicious transactions. However, blockchain forensic tools allow to group public keys attributed to a single subject as well as its counterparties and display them in a figure or graph, which provides a clear picture of

[369] Unità di informazione finanziaria per l'Italia "Prevenzione di fenomeni di criminalità finanziaria connessi con l'emergenza COVID-19", February 2021.
[370] More precisely, the suggestion comes as follows: "Va inoltre considerato che esistono transazioni dirette verso il cosiddetto dark web, indicato recentemente per l'acquisto di prodotti medicinali non sicuri, in genere a fronte della corresponsione di valute virtuali. In proposito, per mitigare il rischio di coinvolgimento in attività illecite e agevolare il riconoscimento di eventuali sospetti, sono senz'altro utili le tecniche di blockchain forensics per l'individuazione di contesti illegali". Ibid, page 5, paragraph 4.
[371] See FATF "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 2019.
[372] Ibid, page 38 and following.
[373] See, for example, *Ciphertrace*.
[374] An alphanumerical string composed of 32 characters and obtained through *sha 256*.

the movements of funds from and to the wallet. It allows to identify patterns that are specific to the money laundering activities.[375]

Such tools enable to group subjects (through *clustering*) that interact with each other and display their transactions graphically. This results to be very useful, for example, for the identification of counterparties in the transactions, before knowing the identity of the subjects initiating the transaction. For example, it underlines whether:

- The subject performs transactions with a highly risky exchange;
- The subject purchase goods and services from e-commerce websites operating in the deep web;
- The subject finances terrorist groups.

Blockchain forensics allows thus to get an understanding of transactions from and to a node.

Instead, money laundering can be detected when a particular pattern, called *Peelchain*: it consists of the performance of a multitude of transactions of low amounts[376] from an exchange to a number of addresses, thus fractioning a considerable sum of cryptocurrency that thanks to Blockchain forensics tools can be again reconstructed in an image. The *Peelchain* technique is similar to that performed by criminals to launder their cash proceeds, which often occurs through currency exchanges.

Blockchain Forensics, used in combination with traditional AML/CFT safeguards, results to be a useful and reliable tool for on-chain[377] inspections.

[375] Such tools are based on algorithms and heuristics which are built on the functioning and characteristics of blockchain, that enable to understand who are the subjects involved in the transaction and identify them.

[376] Lower than the threshold indicated by law for the performance of EDD.

[377] There exist approaches for off-chain analysis that may be useful to use in combination with traditional AML/CFT safeguards and Blockchain Forensics. Such processes allow linking the transactions to wallets through public addresses and pseudonyms to real identities. This is done through the use of open-source intelligence tools able to find public addresses published online, for example in social networks, that may be potentially linked to illicit activities, and thus retrieve users real identities. In fact, a study conducted by Qatar University back in 2017 proved that once users communicate their Bitcoin address online, they risk to be deanonymized.

ANNEX II: DeFi Regulatory Challenges

The crypto asset ecosystem introduced a new paradigm for the financial system through the development of new business models and assets, constituting a growing market.

This new paradigm, as reported by Giuseppe Siani in his Speech for Luiss University,[378] is based on three intertwined dimensions:

- the underlying technology, consisting of DLT;
- the digital representation of value through crypto assets;
- new players operating in a decentralized manner through specific governance mechanisms.

These three dimensions constitute the basis of Decentralized Finance (DeFi).

Decentralized Finance, as its name suggests, is characterized by the lack of a central trusted party, which is instead replaced by a network of nodes taking part in real communities. DeFi is in fact based on permissionless blockchains[379] to which users can freely take part.

Being a central authority ruled out, the mechanisms on which DeFi is based are automated, namely, they make extensive use of smart contracts, which can be defined as pieces of code that automatically executes where certain predetermined conditions are met. Additionally, DeFi does not make use of custodial wallets, thus requiring users to keep their assets in their own wallets.

Interestingly, the blockchain on which DeFi is based, namely permissionless blockchains (of which Ethereum blockchain is an example), allows any developer to create new complex functions based on the original code, which is in fact open-source: these functions are known as dApps, namely Decentralized Applications, which use blockchain-based protocols to operate with little or no human intervention at all.

[378] Speech by Giuseppe Siani, Director General for Financial Supervision and Regulation "Regulating new distributed ledger technologies (DLT): market protection and systemic risks" Luiss Guido Carli University of Rome, May 2022.
[379] As discussed in the first chapter. In this regard, read "Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività", June 2022, page 7.

This open architecture poses unique benefits and risks. For example, according to the *Financial Stability Board*, DeFi may reduce the reliance on existing financial service providers and may help the efficient channeling of resources, in turn reducing traditional providers' solvency and liquidity risks.[380] The pace at which it is developing provided a huge number of use cases, among which, in relation to primary and secondary market asset exchanges. It can be noticed that proponents found effective ways to reach their objective without the need to establish relationships with traditional intermediaries, however posing some issues in terms of governance and legal implications.

In general, most DeFi platforms are established to accomplish a determined business purpose[381] and are intended to operate without a central authority for their command and control. For this reason, those platforms are referred to as Decentralized Autonomous Organizations, "DAOs". This feature raises the point of governance, determined by DeFi protocols which are developed so as to confer upon the code (the smart contract) the governance and responsibility to rule over the community of users.

Typically, where specific conditions are met, the code distributes to participants a determined quantity of a token, also called governance tokens, which gives them the right to participate in the governance decisions with respect to the relevant protocol thanks to which they can propose updates to the platform codebase or simply vote in favor or to discourage a proposed update.

For example, a famous protocol is *MakerDAO*, which consists of a Decentralized Autonomous Organization built on the Ethereum blockchain to allow users to borrow, lend, and exchange digital assets. For instance, users of *MakerDAO* can generate and borrow the "Dai", an algorithmic stablecoin whose market price is algorithmically pegged to the U.S. dollar, in exchange for a deposit of eligible digital assets[382] into a "Vault". The protocol pays interest to those users granting sufficient liquidity such that the value of Dai remains stable and equal to that of the U.S. Dollar.

[380] See FSB "Report on Financial Stability, Regulatory, and Governance Implications of Decentralised Financial Technologies", June 2019, pages 6 and 7.
[381] For example, the facilitation of a peer-to-peer lending transaction.
[382] Typically, Ether.

Another example of protocol DAO is *UNISWAP*, the most famous decentralized exchange. It is built on the Ethereum blockchain too and is built such that order books are replaced by a peer-to-peer system. The liquidity is maintained to a determined level through the *Automated Market Maker*, which provides in real time the asset prices based on the level of the liquidity pool, which is made up of reserves of a pair of two tokens deposited by liquidity providers. When they inject liquidity, they get newly minted liquidity tokens, as well as a proportion of the fee requested to users for completing the transaction.

Liquidity providers can retrieve the underlying liquidity plus any fees accrued by burning[383] their liquidity tokens or by selling them, as they constitute themselves tradable assets.

As mentioned above, DeFi protocols are, in principle, open, immutable, and transparent, and regulators and supervisors may observe them in real-time. However, some limits to the application of regulatory requirements from the platforms exist and make them hail from any regulatory framework. In fact, the reasons for which many present and future (available) rules are not applicable to decentralized platforms lie, above all, in DAOs *decentralized nature.*

The Decentralization issue concretizes in the lack of identification of a single or group of actors that are responsible for the management of the business. In general, it can be noted from Chapters 3 and 4 on the current and upcoming regulatory framework of crypto exchanges, that the regulatory framework in place always refers to a central identifiable entity, thus ruling out decentralized platforms for which no single recognizable central entity (or in form of a group) may be held responsible for the performance and organization of the platform.

For example, as reported in the "FATF Updated Guidance on virtual assets and virtual assets service providers" , "Where it has not been possible to identify a legal or natural person with control or sufficient influence over a DeFi arrangement, there may not be a

[383] Exchanging them for their portion of the liquidity pool.

central owner/operator that meets the definition of a VASP",[384] excluding DAOs from the Obliged Entities list for AML/CFT purposes.

Clearly, the key point lies in whether a DAO that claimed to be decentralized, actually operates without an implicit or explicit reliance on an identifiable responsible party that would benefit financially[385] from the operation of the protocol. Moreover, the governance issue can be raised too: as formerly mentioned, most DAOs make use of governance tokens, which are given to users by the smart contract in exchange for liquidity. Is it possible that the users obtain a large portion of tokens, such that they may be in control of the platform and thus, have a major role in the decisional process?[386] Such questions represent the key for the SEC in determining whether there exists a party that should bear regulatory responsibility for the activities facilitated by the underlying DeFi protocol.

In fact, as pointed out in the Macroprudential bulletin, many "DeFi protocols or platforms claim to have a decentralised governance structure, although in reality governance is often concentrated".[387] The concentration of governance tokens in the hands of few holders may in fact influence the main characteristics of the protocol, and as of today, major holders are represented by developers, early investors or institutional investors, suggesting decentralized DeFi applications retain a high level of centralization instead.[388]

For this reason, Regulators are thinking about possible ways to fill in regulatory gaps, elaborating on how to bring holders of governance tokens, DAOs, and developers into the regulatory perimeter, or, alternatively, to introduce embedded regulation, which

[384] See FATF "Updated Guidance on virtual assets and virtual asset service providers", page 28.
[385] For example, recall the definition of an investment firm brought by the MiFID, which entails that the services and activities should be conducted "as a business".
[386] In this regard, see Lewis Cohen, Angela Angelovska-Wilson, and Greg Strong "Decentralized Finance: Have digital assets and open blockchain networks found their "killer app"?", Global Legal Insight 2021, page 134.
[387] See A. Born, I. Gschossmann, A. Hodbod, C. Lambert and A. Pellicani, "Decentralised finance – a new unregulated non-bank system?", ECB Macroprudential Bulletin.
[388] Ibid. The Bulletin highlights that, for example, 80% of the total supply in circulation of UNISWAP's Uni is held by the Uniswap team, early investors and holders with huge balances.

would require the creation of a technology-based regulatory system technically embedded in DeFi.

In this regard, experts[389] from the field claim that the introduction of a regulatory regime in the field may suffocate innovation, being unfavorable for the development of DAOs.

[389] "Il Regolamento Market in Crypto Asset – Discussione Pubblica sul futuro della regolamentazione Europea MiCA". Discussion panel with Stefano Capaccioli, Massimiliano Nicotra, Andrea Pantaleo, Claudia Morelli, Tamara Belardi, Martina Granatiero, Marco Tullio Giordano, Sara Noggler e Davide Zanichelli.

ANNEX III: A new Definition of Financial Instrument

Following the Russian invasion of Ukraine in February 2022, a number of sanctions have been imposed on Russia, among which targeted restrictive measures, economic sanctions, and diplomatic measures.

In particular, the economic sanctions aim is that of imposing severe consequences on Russia in order to contrast Russian abilities to continue the attacks.

The Financial Sector is impacted in three ways:

- Transactions with the Russian Central Bank and the Central Bank of Belarus are prohibited;
- A ban is imposed on some Russian and Belarus banks from SWIFT;[390]
- Access to capital markets is restricted for some Russian banks and companies.

In order to limit the money transfers to Russia, the Russian Central Banks has been impacted via SWIFT. More specifically, a ban[391] is imposed on ten Russian and four Belarusian banks from making or receiving international payments using SWIFT.

SWIFT consists of a messaging service that facilitates information exchange between banks and other financial institutions and connects more than 11000 entities worldwide. It is not a payment system, however, it makes payment systems largely dependent on it. In fact, the ban implies that the indicated banks are not able to get foreign currency and cannot transfer assets abroad, for which the two countries' economies are subject to negative consequences.[392]

---

[390] Which is the global provider of secure financial messaging services.

[391] *Article 5h* of "Council Regulation (EU) 2022/345 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine" states that "'It shall be prohibited as of 12 March 2022 to provide specialised financial messaging services, which are used to exchange financial data, to the legal persons, entities or bodies listed in Annex XIV or to any legal person, entity or body established in Russia whose proprietary rights are directly or indirectly owned for more than 50 % by an entity listed in Annex XIV". This restriction was subsequently extended to Belarus.

[392] Banks can carry out international transactions without SWIFT, but in a more expensive and complex way.

The exclusion from SWIFT caused the disconnection of the banned banks from the international financial system, preventing them from operating globally.[393]

Of course, some features of the sanctions made clear that there could exist some ways to circumvent the law. First, the sanctions affect the banks listed in Annex XIV of the "Council Regulation (EU) 2022/345 of 1 March 2022 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine" do not address branches and subsidiaries present in the European Union territory, raising doubts on the fact that such entities might in fact use SWIFT for the Russian and Belarusian Banks. However, Russian banks may join the *Cross-Border Interbank Payment System*[394], an information platform for Chinese payments which only processes transactions in Yuan. Additionally, the Russian Central Banks developed an alternative messaging platform, the *System for Transfer of Financial Messages*,[395] for Russian residents' transactions.

However, market prices at the end of February suggested Russian citizens were seeking to circumvent the law using alternative, less traditional means that would not involve banks: crypto assets. For instance, Bitcoin registered +16%[396] at the beginning of March, alarming Authorities as the regulatory framework in this field is currently much fragmented.

As explained in the previous chapters, the application of rules, for example, the MiFID, is related to the legal characterization of crypto assets, for which an attentive case-by-case analysis should be conducted.

Interestingly, the sanctions subsequently imposed with the Council Regulation,[397] prohibit Member States to "directly or indirectly purchase, sell, provide investment services for or assistance in the issuance of, or otherwise deal with transferable securities and money-market instruments […] issued by (a) a major credit institution, or

[393] As reported in the European Commission Joint Statement on further restrictive economic measures of February 2022.
[394] CIPS.
[395] SPFS.
[396] Read Arjun Kharpal, "Bitcoin jumps as Russia-Ukraine conflict continues and U.S. imposes further sanctions" CNBC, March 2022.
[397] See "Council Regulation (EU) 2022/394 of 9 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine" ST (2022) 6973 INIT.

other major institution having an explicit mandate to promote competitiveness of the Russian economy, its diversification, and encouragement of investment, established in Russia with over 50 % public ownership or control as of 1 August 2014, as listed in Annex III; or (b) a legal person, entity or body established outside the Union whose proprietary rights are directly or indirectly owned for more than 50 % by an entity listed in Annex III; or (c) a legal person, entity or body acting on behalf or at the direction of an entity referred to in point (b) of this paragraph or listed in Annex III",[398] as well as those issued by "(a) Russia and its government; or (b) the Central Bank of Russia; or (c) a legal person, entity or body acting on behalf or at the direction of the entity referred to in point (b)".[399]

It is understood that some crypto assets fall under the definition of financial instruments,[400] particularly when they fall under the definition of transferable security.[401]

However, interestingly, the regulator also declared that "Whereas it is commonly understood that loans and credits can be provided by any means, including crypto assets, given their specific nature it is appropriate to further specify the notion of "transferable securities" in relation to such assets".[402]

Thus, the Council regulation was amended as follows:

"(1) in Article 1, the introductory words of point (f) are replaced by the following:

[398] Ibid, Article 5.
[399] Ibid, Article 5e.
[400] From Chapter 3.
[401] Recall that "transferable securities means the following classes of securities which are negotiable on the capital market, with the exception of instruments of payment: (i) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares, (ii) bonds or other forms of securitised debt, including depositary receipts in respect of such securities, (iii) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities".
[402] Recital 4 of Council Regulation (EU) 2022/394 of 9 March 2022 (see footnote 397).

‘(f) “transferable securities means the following classes of securities, including in the form of crypto-assets, which are negotiable on the capital market, with the exception of instruments of payment”.[403]

The prohibitions in relation to crypto assets were expanded in April 2022, with the Council Decision,[404] whose sixth recital proposes the introduction of further restrictive measures, among to extend the prohibition on deposits to crypto wallets.

In fact, Article 1b disposed that “It shall be prohibited to provide crypto-asset wallet, account or custody services to Russian nationals or natural persons residing in Russia, or legal persons, entities or bodies established in Russia, if the total value of crypto-assets of the natural or legal person, entity or body per wallet, account or custody provider exceeds EUR 10 000”.

With the introduction of prohibitions for high-value crypto asset services to persons and entities in Russia, the European Union aim was to contribute to the closing potential loopholes.[405]

With the Sanctions imposed on Russia and Belarus, it can be noted that, firstly, measures were extended from traditional finance to crypto assets, but above all, that the regulator included *explicitly* crypto assets within the *financial instruments* definition.

The legal characterization of crypto assets requires quite a complex analysis, and often ends up leaving most assets outside the regulatory perimeter, raising regulatory arbitrage and legal uncertainty, which are exacerbated by the different transposition of Directives across jurisdictions.

The explicit inclusion of crypto assets among Financial Instruments may be quite controversial thinking about the ongoing debate on the definition of a defined legal perimeter but also raises a question: *does it constitute a new, possible definition of financial instrument?*

---

[403] Ibid.

[404] See “Council Decision (CFSP) 2022/578 of 8 April 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine” ST (2022) 7900 INIT.

[405] Read the European Commission “Question and answers on the fifth package of restrictive measures against Russia of April 2022”.

References

Annunziata F. “Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE”. Diritto Bancario, October 2020.
Available at: https://www.dirittobancario.it/art/verso-una-disciplina-europea-delle-cripto-attivita-riflessioni-margine-recente-proposta-commissione/

Annunziata F., Conso A., Di Giorgio A., Lucchini A., Seri L.M., Carozzi M., Borsa P., Braccioni P., NFT L’arte e il suo doppio – non fungible token: l’importanza delle regole oltre i confini dell’arte. Montabone, Ottobre 2021.

Annunziata F., Minto A., “Il nuovo Regolamento UE in materia di Distributed Ledger Technology - Analisi del nuovo DLT Pilot Regime”, Diritto Bancario, July 2022.
Available at: https://www.dirittobancario.it/art/il-nuovo-regolamento-ue-in-materia-di-distributed-ledger-technology/

Annunziata&Conso “Decreto ministeriale 13 gennaio 2022 sulle modalità e tempistiche di comunicazione di operatività all’OAM da parte dei prestatori di servizi relativo all’utilizzo di valuta virtuale e dei prestatori di servizi di portafoglio digitale”, PILL n. 01–2022, February 2022.
Available at: https://annunziataconso.eu/it/decreto-ministeriale-13-gennaio-2022-sulle-modalita-e-tempistiche-di-comunicazione-di-operativita-alloam-da-parte-dei-prestatori-di-servizi-relativi-allutilizzo-di-valuta-virtuale-e/

Annunziata, F. “Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings”, February 2019.
Available at SSRN: https://ssrn.com/abstract=3332485

Aramonte S., Huang W. and Schrimpf A., “Trading in the DeFi era: automated market-maker”. Bank for International Settlements, December 2021.
Available at: https://www.bis.org/publ/qtrpdf/r_qt2112v.htm

Autorité des Marchés Financiers “Obtaining a DASP registration/optional licensing”, July 2022.
Available at: https://www.amf-france.org/en/professionals/fintech/my-relations-amf/obtain-dasp-authorisation#In_which_cases_is_registration_with_the_AMF_mandatory_

Autorité des Marchés Financiers “Questions and Answers on the DASP Regime”.
Available at: https://www.amf-france.org/en/regulation/policy/doc-2020-07

Autorité des Marchés Financiers "The AMF publishes a discussion paper on Initial Coin Offerings and initiates its UNICORN programme", October 2017.
Available at: https://www.amf-france.org/en/news-publications/news-releases/amf-news-releases/amf-publishes-discussion-paper-initial-coin-offerings-and-initiates-its-unicorn-programme

Autorité des Marchés Financiers, "Obtaining a DASP registration/optional licensing, September 2022.
Available at: https://www.amf-france.org/en/professionals/fintech/my-relations-amf/obtain-dasp-authorisation#In_which_cases_is_registration_with_the_AMF_mandatory

Autorité des Marchés Financiers, "Questions & answers on the digital asset service providers regime".
Available at: https://www.amf-france.org/sites/default/files/private/2022-06/doc-2020-07_eng.pdf

Autorité des Marchés Financiers, "Towards a new regime for crypto-assets in France", April 2019, News section.
Available at: https://www.amf-france.org/en/news-publications/news/towards-new-regime-crypto-assets-france

Banca d'Italia "Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività", June 2022.
Available at: https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf

Benfedda R., Bourran E., "PSAN : l'AMF précise sa doctrine pour 2022", Beaubourg Avocats.
Available at: https://beaubourg-avocats.fr/psan-amf/

Berruto A., "La nuova disciplina francese dei crypto-asset: un imperfetto tentativo regolatorio?" February 2020.
Available at: https://www.dirittobancario.it/art/la-nuova-disciplina-francese-dei-crypto-asset-un-imperfetto-tentativo-regolatorio/

Betz B., "Binance Resumes Bitcoin Withdrawals After Pause", CoinDesk, 14 June 2022.
Available at: https://www.coindesk.com/business/2022/06/13/binance-temporarily-pauses-bitcoin-withdrawals/

Binance “CZ FAQ 5 - Why Binance Embraces Regulations”, Binance Blog, July 2022. Available at: https://www.binance.com/en/blog/from-cz/cz-faq-5--why-binance-embraces-regulations-421499824684903224

Born A., Gschossmann I., Hodbod A., Lambert C. and Pellicani A., “Decentralised finance – a new unregulated non-bank system?” ECB Macroprudential Bulletin.
Available at: https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html

Busuttil I., “The MFSA issues Consultation Paper on proposed Financial Instrument Test applicable to DLT assets”. Mamo TCV Advocates, April 2018.
Available at: https://www.mamotcv.com/insights/the-mfsa-issues-consultation-paper-on-proposed-financial-instrument-test-applicable-to-dlt-assets/

Cavicchioli, M., “Mt. Gox si sta preparando ad effettuare i rimborsi”, The Cryptonomist, Sempember 2022.
Available at: https://cryptonomist.ch/2022/09/01/mt-gox-effettua-rimborsi/

Cavin C., Chiriaeva M., Poskriakov F., “Cryptocurrency compliance and risks: A European KYC/AML perspective”. 2021 Global Legal Insights (GLI) Blockchain & Cryptocurrency Regulation.
Available at: https://www.acc.com/sites/default/files/resources/upload/GLI-BLCH21_E-Edition.pdf

Chainalysis “Crypto Money Laundering: How Criminals Cash Out Billions in Bitcoin and Other Cryptocurrencies”, January 2020.
Available at: https://blog.chainalysis.com/reports/crypto-money-laundering-2019/

Chetcuti Cauchi M., “Anti-money laundering legislation in Malta”. Chetcuti Cauchi Advocates, September 2019.
Available at: https://www.ccmalta.com/publications/malta_anti_money_laundering

Chimienti M.T., Kochanska U. and Pinna A., “Understanding the crypto-asset phenomenon, its risks and measurement issues”, ECB Economic Bulletin, May 2019. Available at: https://www.ecb.europa.eu//pub/economic-bulletin/articles/2019/html/ecb.ebart201905_03~c83aeaa44c.en.html?utm_source=ecb_twitter&utm_medium=social&utm_campaign=190808_eb_5_2019&utm_term=cryptoassets#toc1

Ciphertrace, Cryptocurrency intelligence & blockchain analytics.
Available at: https://ciphertrace.com/

Code monétaire et financier.
Available at: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006072026/

Cohen L., Angelovska-Wilson A., Strong G. “Decentralized Finance: Have digital assets and open blockchain networks found their “killer app”?”, Global Legal Insight 2021.
Available at: https://www.acc.com/sites/default/files/resources/upload/GLI-BLCH21_E-Edition.pdf

CoinMarketCap “Top Cryptocurrency Spot Exchanges”. Available at: https://coinmarketcap.com/rankings/exchanges/

CONSOB “Le criprovalute”. Available at: https://www.consob.it/web/investor-education/criptovalute

CONSOB, “Le offerte iniziali e gli scambi di cripto-attività Rapporto finale”, January 2020.
Available at: https://www.consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.pdf/70466207-edb2-4b0f-ac35-dd8449a4baf1

CONSOB, “Le offerte iniziali e gli scambi di cripto-attività. Documento per la Discussione” March 2019.
Available at: https://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/12117302-78b0-4e6e-80c4-d3af7db0fdae

De N., “Crypto Lending Service Celsius Pauses Withdrawals, Citing 'Extreme Market Conditions'”, CoinDesk, 14 June 2022.
Available at: https://www.coindesk.com/policy/2022/06/13/crypto-lending-service-celsius-pauses-withdrawals-citing-extreme-market-conditions/

Decreto Legislativo 21 novembre 2007, n. 231, “Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché' della direttiva 2006/70/CE che ne reca misure di esecuzione”. Available at: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2007-11-21;231!vig=

Decreto legislativo 24 febbraio 1998, n. 58 “Testo Unico della Finanza”. Available at: https://www.consob.it/documents/46180/46181/dlgs58_1998.pdf/e15d5dd6-7914-4e9f-959f-2f3b88400f88

Decreto legislativo del 13/08/2010 n. 141 “Attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori, nonché' modifiche del titolo VI del testo unico bancario (decreto legislativo n. 385 del 1993) in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi”.
Available at: https://def.finanze.it/DocTribFrontend/getAttoNormativoDetail.do?ACTION=getSommario&id={CB942277-2A06-4D5A-BE3F-66899185F49C}

Deutsche Bundesbank “Distributed ledger technologies in payments and securities settlement: potential and risks” Deutsche Bundesbank Monthly Report, September 2017.
Available at: https://www.bundesbank.de/resource/blob/707710/3f3bd66e8c8a0fbeb745886b3f072b15/mL/2017-09-distributed-data.pdf

Di Giorgio A., Lucchini A., “Prime considerazioni sul Decreto sui prestatori di servizi di valuta virtuale e portafoglio digitale”, Diritto Bancario, February 2018.
Available at: https://www.dirittobancario.it/art/prime-considerazioni-sul-decreto-sui-prestatori-di-servizi-di-valuta-virtuale-e-portafoglio-digitale/

Diritto Bancario “Crypto-asset: il Regolamento UE sulla distributed ledger technology”, June 2022.
Available at: https://www.dirittobancario.it/art/crypto-asset-il-regolamento-ue-sulla-distributed-ledger-technology/

European Banking Authority “Anti-Money laundering and Countering the Financing of Terrorism”, Factsheet.
Available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20acts%20to%20improve%20AML/CFT%20supervision%20in%20Europe/AML%20CFT%20Factsheet.pdf

European Banking Authority “EBA warns consumers on virtual currencies” EBA Warning, December 2013.
Available at: https://www.eba.europa.eu/eba-warns-consumers-on-virtual-currencies

European Banking Authority “Opinion of the European Banking Authority on the EU Commission’s proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD), August 2016”.

Available at: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1547217/32b1f7f2-90ec-44a8-9aab-021b35d1f1f7/EBA%2520Opinion%2520on%2520the%2520Commission%25E2%2580%2599s%2520proposal%2520to%2520bring%2520virtual%2520currency%2520entities%2520into%2520the%2520scope%2520of%25204AMLD.pdf?retry=1

European Banking Authority "Report with advice for the European Commission on crypto-assets", January 2019.
Available at: EBA Report on crypto assets.pdf (europa.eu)

European Central Bank "ECB Financial Stability Review 2022", May 2022.
Available at: https://www.ecb.europa.eu/pub/financial-stability/fsr/html/ecb.fsr202205~f207f46ea0.en.html

European Central Bank "Our retail payments strategy".
Available at: https://www.ecb.europa.eu/paym/integration/retail/retail_payments_strategy/html/index.en.html

European Commission "Anti-money laundering and countering the financing of terrorism legislative package".
Available at: https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en

European Commission "Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules".
Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

European Commission "Commission Staff Working Document – Executive Summary of the impact assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937".
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0381

European Commission "Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06" C (2020) 2800.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0513(03)

European Commission “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU” COM (2020) 591 final.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591

European Commission “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's digital future”.
Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067

European Commission “Communication from the Commission to the European Parliament, the Council, the European Central Bank the European Economic and Social Committee and the Committee of the Regions on a FinTech Action plan: For a more competitive and innovative European financial sector”. COM (2018) 109 final.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109

European Commission “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU”.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0592

European Commission “Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses”, Press Release, September 2020.
Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

European Commission “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”.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L2366-20151223

European Commission “Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No

648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC".
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

European Commission "Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC".
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02009L0110-20180113

European Commission "Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU".
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0065-20220228

European Commission "Joint Statement on further restrictive economic measures", February 2022.
Available at: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_1423

European Commission "Opening remarks by Commissioner McGuinness at the ECON Committee Structured Dialogue", June 2022.
Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_3702

European Commission "Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849". COM (2021) 423 final.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423

European Commission "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937" COM (2020) 593 final.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593&qid=1661525391451

European Commission “Proposal for a Regulation of the European Parliament and of 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 final.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0595

European Commission “Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010”.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0421

European Commission “Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing”. COM (2021) 420 final.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420

European Commission “Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets”.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422

European Commission “Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)”.
Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_3689

European Commission “Questions and Answers: Digital Finance Strategy, legislative proposals on crypto-assets and digital operational resilience, Retail Payments Strategy”, September 2020.
Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1685

European Commission “Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006”.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015R0847-20200101

European Commission “Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on

distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU".
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0858

European Commission "Digital Finance Package", September 2020. Available at: https://finance.ec.europa.eu/publications/digital-finance-package_en

European Commission, "A Digital Finance Strategy for Europe" Factsheet, September 2020.
Available at: https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-digital-finance-factsheet_en.pdf

European Commission, "Anti-money laundering and countering the financing of terrorism, Fighting money laundering and terrorist financing contributes to global security, integrity of the financial system and sustainable growth, Latest Developments and EU context".
Available at: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en

European Commission, "EU context of anti-money laundering and countering the financing of terrorism".
Available at: https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en

European Commission, "Investment services and regulated markets - Markets in financial instruments directive (MiFID)".
Available at: https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/financial-markets/securities-markets/investment-services-and-regulated-markets-markets-financial-instruments-directive-mifid_en

European Commission, "Question and answers on the fifth package of restrictive measures against Russia", March 2022.
Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_2333

European Commission, "Strengthened EU rules to prevent money laundering and terrorism financing, Factsheet on the main changes of the 5th Anti-Money Laundering Directive".

Available at: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en#documents

European Commission: "FinTech: Commission takes action for a more competitive and innovative financial market", Press Release, March 2018.
Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_1403

European Commission "Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing". COM (2016) 050 final.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1455113825366&uri=CELEX:52016DC0050#footnote9

European Council "Council Regulation (EU) 2022/345 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine".
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.063.01.0001.01.ENG

European Council "Council Regulation (EU) 2022/394 of 9 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine".
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0394

European Council "Decision (CFSP) 2022/578 of 8 April 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine".
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.111.01.0070.01.ENG&toc=OJ%3AL%3A2022%3A111%3ATOC

European Council "Digital finance: agreement reached on European crypto-assets regulation (MiCA)". Press release, June 2022.
Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

European Council, “EU sanctions against Russia explained”. Available at: https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/

European Securities and Markets Authority “Advice on Initial Coin Offerings and Crypto-Asset”, January 2019.
Available at: esma50-157-1391_crypto_advice.pdf (europa.eu)

European Securities and Markets Authority “ESMA assesses usefulness of Distributed Ledger Technologies”, June 2016.
Available at: https://www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies

European Securities and Markets Authority “Report - The Distributed Ledger Technology Applied to Securities Markets”, February 2017.
Available at: https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

European Securities and Markets Authority, Financial and Technological Innovation. Available at: https://www.esma.europa.eu/risk-analysis/financial-and-technological-innovation

European Supervisory Authorities “Crypto-assets: ESAs remind consumers about risks. ESAs Publication”, March 2021.
Available at: https://www.eba.europa.eu/financial-innovation-and-fintech/publications-on-financial-innovation/crypto-assets-esas-remind-consumers-about-risks

European Supervisory Authorities “ESAs warn consumers of risks in buying virtual currencies”. ESAs Warning, February 2018.
Available at: https://www.eba.europa.eu/esas-warn-consumers-of-risks-in-buying-virtual-currencies

European Supervisory Authorities “EU financial regulators warn consumers on the risks of crypto-assets”. ESAs Warning, March 2022.
Available at: https://www.eba.europa.eu/eu-financial-regulators-warn-consumers-risks-crypto-assets

European Supervisory Authorities “Joint Advice of the European Supervisory Authorities To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector”.

Available at: https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf)

European Supervisory Authorities "Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice on digital finance and related issues" January 2022.
Available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2022/1026595/ESA%202022%2001%20ESA%20Final%20Report%20on%20Digital%20Finance.pdf

Financial Action Task Force "Easy Guide to FATF Standards and Methodology – Virtual Assets: What, When, How?"
Available at: https://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf

Financial Action Task Force "FATF Report on Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing" September 2020.
Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

Financial Action Task Force "Second 12-month review on the revised FATF standards on virtual assets and virtual assets service providers", July 2021.
Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

Financial Action Task Force "Updated Guidance for a Risk-Based Approach Virtual Assets and Virtual Asset Service Providers" October 2021.
Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

Financial Stability Board "Final Report and High-Level Recommendations 2020, Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements".
Available at: https://www.fsb.org/wp-content/uploads/P131020-3.pdf

Financial Stability Board "FinTech".
Available at: https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech/

Financial Stability Board “Report on Financial Stability, Regulatory, and Governance Implications of Decentralised Financial Technologies”, June 2019.
Available at: https://www.fsb.org/wp-content/uploads/P060619.pdf

Financial Stability Board, “Assessment of Risks to Financial Stability from Crypto-assets”. February 2022.
Available at: https://www.fsb.org/wp-content/uploads/P160222.pdf

Financial Stability Board, “Crypto-asset markets Potential channels for future financial stability implications”, October 2018.
Available at: https://www.fsb.org/wp-content/uploads/P101018.pdf

FINMA “FINMA Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)” February 2018.
Available at: https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?sc_lang=en&hash=C9899ACF22747D56C800C6C41A7E28AB

Foley S., R. Karlsen J., J. Putniņš T., “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?”, The Review of Financial Studies, Volume 32, Issue 5, May 2019, Pages 1798–1853.
Available at : https://doi.org/10.1093/rfs/hhz015

Forbes “15 Industries That Could Significantly Benefit From Blockchain Technology”. Available at: https://www.forbes.com/sites/forbestechcouncil/2022/06/10/15-industries-that-could-significantly-benefit-from-blockchain-technology/?sh=e42976c7af21

Ganado Advocates “Snapshot Summary Of Three Bills Related to Blockchain Technology”, June 2018.
Available at: Snapshot Summary Of Three Bills Related to Blockchain Technology - Ganado Advocates

Gartner, “Smart contracts” Information Technology Glossary. Available at: https://www.gartner.com/en/information-technology/glossary/smart-contract

Gazzetta Ufficiale della Repubblica Italiana, Anno 163°, numero 40 “Decreto 13 gennaio 2022, Modalità e tempistica con cui i prestatori di servizi relativi all’utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria

operatività sul territorio nazionale nonché forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia".
Available at: https://www.gazzettaufficiale.it/eli/gu/2022/02/17/40/sg/pdf

Gouvernement Français "PACTE : un plan d'action pour la croissance et la transformation des entreprises", December 2017.
Available at : https://www.gouvernement.fr/argumentaire/pacte-un-plan-d-action-pour-la-croissance-et-la-transformation-des-entreprises

Hermans L., Ianiro A., Kochanska U., Törmälehto V.M., van der Kraaij A., Vendrell Simon J.M., "Decrypting financial stability risks in crypto-asset markets". Financial Stability Review, ECB Publications.
Available at: https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202205_02~1cc6b111b4.en.html

Horobin W. "Crypto Shows All the Signs of Financial Stability Risk, ECB Says". Bloomberg, May 2022.Available at: https://www.bloomberg.com/news/articles/2022-05-24/crypto-shows-all-the-signs-of-financial-stability-risk-ecb-says?leadSource=uverify%20wall

IBM, "Blockchain for Industries".
Available at: https://www.ibm.com/blockchain/industries

IBM, "Benefits of blockchain".
Available at: https://www.ibm.com/topics/benefits-of-blockchain

Initial Virtual Financial Asset Offerings Act, July 2018.
Available at: https://legislation.mt/eli/act/2018/30/eng/pdf

IOSCO, "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms - Final Report" February 2020.
Available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf

Kharpal A., "Bitcoin jumps as Russia-Ukraine conflict continues and U.S. imposes further sanctions". CNBC, March 2022.
Available at: https://www.cnbc.com/2022/03/01/bitcoin-btc-price-jumps-as-russia-ukraine-conflict-continues.html

KPMG "Crypto Insights #2. Decentralised Exchanges & Automated Market Makers – Innovations, Challenges & Prospects", October 2021.

Available at: https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2021/10/crypto-insights-part-2-decentralised-exchanges-and-automated-market-makers.pdf

Lipusch N., Dellermann, D., Ebel P., Ghazawneh A., Leimeister J.M., "Token-Exchanges as a Mechanism to Create and Scale Blockchain Platform Ecosystems", August 2019. Available at: https://ssrn.com/abstract=3434941

Luini F., "MiCA: Il rischio di un regolamento nato 'vecchio'", Luglio 2022, FUNDSPEOPLE. Available at: https://fundspeople.com/it/mica-il-rischio-di-un-regolamento-nato-vecchio/

Maltese Virtual Financial Assets Act, Chapter 590.
Available at: https://www.mfsa.mt/wp-content/uploads/2018/12/fintech-main-legislation.pdf

MFSA Virtual Financial Assets, "Understanding the VFA Framework".
Available at: https://www.mfsa.mt/our-work/virtual-financial-assets/)

Mifsud Parker P., Vassallo S., "World 1st Comprehensive DLT Legislation enacted in Malta". Chetcuti Cauchi Advocates, July 2018.
Available at: https://www.ccmalta.com/news/malta-blockchain-crypto-legislation

Minto A., "The Legal Characterization of Crypto-Exchange Platforms" Global Jurist, vol. 22, no. 1, 2022, pp. 137-156.
Available at: https://doi.org/10.1515/gj-2020-0085

Nakamoto S., "A Peer-to-Peer Electronic Cash System", 2008.
Available at: https://bitcoin.org/bitcoin.pdf)

Nakamura Y., Tan A., "Massive Cryptocurrency Heist Spurs Call for More Regulation". Bloomberg Crypto, January 2018.
Available at: https://www.bloomberg.com/news/articles/2018-01-28/massive-cryptocurrency-heist-puts-spotlight-on-exchange-security

O'Rorke, W., Lourimi, A., "Blockchain and Cryptocurrency Laws and Regulations 2022, France". Global Legal Insights 2022.
Available at: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/france

Orcutt, M. “Criminals laundered $2.8 billion in 2019 using crypto exchanges, finds a new analysis”, MIT Technology Review, January 2020.
Available at: https://www.technologyreview.com/2020/01/16/130843/cryptocurrency-money-laundering-exchanges/

Organismo Agenti e Mediatori, “Vademecum Operatori Valute Virtuali”.
Available at: https://www.organismo-am.it/vademecum-vasp

Organismo Agenti e Mediatori, Elenchi e Servizi. Ù
Available at: https://www.organismo-am.it/elenchi-e-registri-in-manutenzione/

Panetta F. “For a few cryptos more: the Wild West of crypto finance”. Speech at Columbia University, April 2022.
Available at: https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220425~6436006db0.en.html
Paz J., “The Best Global Crypto Exchanges”. Forbes, March 2022.
Available at: https://www.forbes.com/sites/javierpaz/2022/03/16/the-best-global-crypto-exchanges/?sh=71f004a3742c

Portale V., “La proposta MiCAR: sfida normativa per lo sviluppo del mercato Crypto - La proposta di regolamentazione focalizzata sul mercato dei crypto-asset: la Markets in Crypto-assets Regulation”. Novembre 2021, Il Sole 24 Ore Finanza.
Available at: https://www.ilsole24ore.com/art/la-proposta-micar-sfida-normativa-lo-sviluppo-mercato-crypto-AEXe5ZUB

Quarta L., “Il MiCA è stato ufficialmente approvato”. The Cryptonomist, July 2022.
Available at: https://cryptonomist.ch/2022/07/01/mica-ufficialmente-approvato/

Siani G., “Regulating new distributed ledger technologies (DLT): market protection and systemic risks” Speech at Luiss Guido Carli University, May 2022.
Available at: https://www.bancaditalia.it/pubblicazioni/interventi-vari/int-var-2022/en_SIANI_3_maggio_2022.pdf?language_id=1

Stimolo, S., “The Differences between Blockchain and Distributed Ledger Technology (DLT)”, the Cryptonomist, November 2018.
Available at: https://en.cryptonomist.ch/2018/11/25/differences-blockchain-distributed-ledger-technology-dlt/

Unità di Informazione Finanziaria per l’Italia “Prevenzione di fenomeni di criminalità finanziaria connessi con l'emergenza da COVID-19” 11 febbraio 2021.

Available at: https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione-UIF-Covid-19-110221.pdf

Unità di Informazione Finanziaria per l'Italia, "Sviluppi Europei. L'AML Package". Newsletter, May 2021.

Available at: https://uif.bancaditalia.it/pubblicazioni/newsletter/2021/newsletter-2021-5/newsletter-21-V.pdf

Wood J., "Custodial Wallets vs. Non-Custodial Crypto Wallets", CoinDesk Crypto Explainer.
Available at: https://www.coindesk.com/learn/custodial-wallets-vs-non-custodial-crypto-wallets/

Zetzsche A., Dirk A., Annunziata F. Arner D.W., Buckley R.P., "The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy" November 2020. Available at SSRN: https://ssrn.com/abstract=3725395