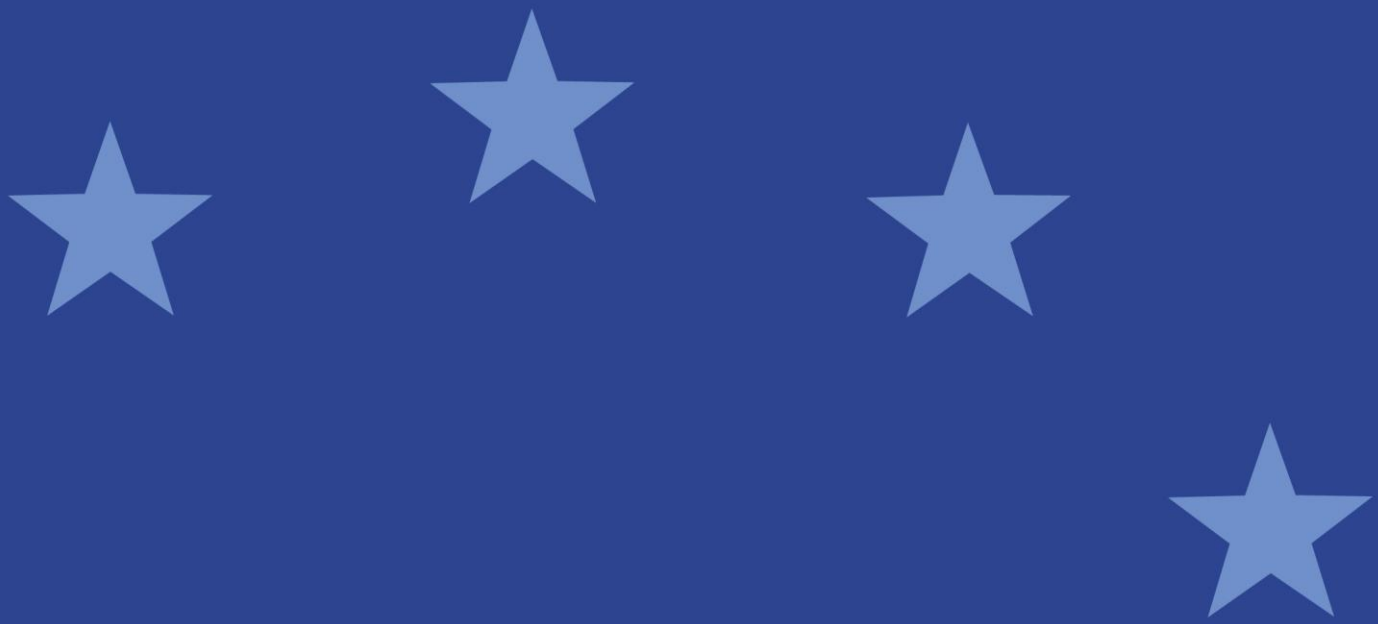
esma European Securities and Markets Authority

Advice

Initial Coin Offerings and Crypto-Assets



9 January 2019 | ESMA50-157-1391

Table of Contents

I. Executive summary

1. Crypto-assets are a type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT). There are a wide variety of crypto-assets. Examples of crypto-assets range from so-called cryptocurrencies or virtual currencies, like Bitcoin, to so-called digital tokens issued through Initial Coin Offerings (ICOs). Some crypto-assets have attached profit or governance rights while others provide some consumption value. Still others are meant to be used as a means of exchange. Many have hybrid features. Crypto-assets are relatively new and the market is evolving. There are more than 2,000 crypto-assets outstanding.

2. Crypto-assets raise specific challenges for regulators and market participants, as there may be a lack of clarity as to how the regulatory framework applies to such instruments. Where it does apply, there may be areas where crypto-assets require potential interpretation or re-consideration of specific requirements to allow an effective application of regulations. Where regulation does not apply to crypto-assets and related activities, regulators need to consider whether it should, and if so how. ESMA considers it important to take a technology-neutral approach, to ensure that similar activities and assets are subject to the same or very similar standards regardless of their form.

3. In its 2018 FinTech Action plan, the European Commission requested the European Supervisory Authorities (ESAs) assess the suitability of the EU regulatory framework with regards to ICOs and crypto-assets more generally.[1]

4. The crypto-assets sector remains modest in size and ESMA does not believe that it currently raises financial stability issues. However, ESMA is concerned about the risks it poses to investor protection and market integrity. ESMA identifies the most significant risks as fraud, cyber-attacks, money laundering, and market manipulation. Meanwhile, there could be benefits in ICOs provided the appropriate safeguards are in place. The development of tokenisation, i.e., the representation of traditional assets on DLT, could bring benefits, although it is still at a very early stage. Crypto-assets are one application of DLT. ESMA sees a number of potential benefits in DLT but there are important challenges as highlighted in our 2017 DLT report.[2]

5. A key consideration for regulators is the legal status of crypto-assets, as this determines whether financial services rules are likely to apply, and if so which, and hence the level of protection to investors. Because the range of crypto-assets are diverse and many have hybrid features, ESMA believes that there is not a 'one size fits all' solution when it comes to legal qualification. To better understand the circumstances under which crypto-assets may qualify as financial instruments in the EU, ESMA undertook a survey

[1] European Commission, 2018. 'FinTech Action plan: for a more competitive and innovative European financial sector', March 2018. Available at https://ec.europa.eu/info/publications/180308-action-plan-fintech_en

[2] ESMA, 2017. 'The Distributed Ledger Technology Applied to Securities Markets', February 2017. Available at https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf

of National Competent Authorities (NCAs) of Member States in the summer of 2018, using a sample set of crypto-assets. The sample crypto-assets were real crypto-assets that may be available to European investors. They reflected differing characteristics that ranged from investment-type, to utility-type, and hybrids of investment-type, utility-type and payment-type crypto-assets. Pure payment-type crypto-assets were not included in the sample set on purpose as they are unlikely to qualify as financial instruments.

6. The outcome of the survey highlighted a NCA majority view that some crypto-assets, e.g. those with profit rights attached, may qualify as transferable securities or other types of MiFID financial instruments. The actual classification of a crypto-asset as a financial instrument is the responsibility of an individual NCA and will depend on the specific national implementation of EU law and the information and evidence provided to that NCA. The results of the Survey made clear that the Member State NCAs in the course of transposing MiFID into their national laws, have in turn defined the term financial instrument differently. While some employ a restrictive list of examples to define transferable securities, others use broader interpretations. This creates challenges to both the regulation and to the supervision of crypto-assets.

7. Where crypto-assets qualify as transferable securities or other types of MiFID financial instruments, a full set of EU financial rules, including 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, are likely to apply to their issuer and/or firms providing investment services/activities to those instruments. However, ESMA has identified a number of gaps and issues in the existing regulatory framework when applied to crypto-assets. In particular, some of the risks that are specific to their underlying technology may be left unaddressed. Meanwhile certain existing requirements may not be easily applied or may not be entirely relevant in a DLT framework.

8. Where crypto-assets do not qualify as financial instruments (or where they do not fall within the scope of other EU rules applicable to non-financial instruments such as the e-money directive as identified in the EBA's report and advice on crypto-assets[3]), ESMA believes that the absence of applicable financial rules leaves consumers exposed to substantial risks. ESMA believes that EU policymakers should consider possible ways to address the risks in a proportionate manner. Also, ESMA believes that all crypto-assets and related activities should be subject to AML provisions (on which see further the EBA's report and advice on crypto-assets)[4].

9. ESMA has noted that some Member States have or are considering some bespoke rules at the national level for all or a subset of those crypto-assets that do not qualify as MiFID financial instruments. While ESMA understands the intention to bring to the topic both a protective and supportive approach, ESMA is concerned that this does not provide for a level playing field across the EU. ESMA believes that an EU-wide approach is relevant, also considering the cross-border nature of crypto-assets.

[3] EBA, 2019. 'Report with advice for the European Commission on crypto-assets', January 2019.
[4] See footnote 3

10. This Advice outlines ESMA's position on the gaps and issues that exist in the rules within ESMA's remit when crypto-assets qualify as financial instruments and the risks that are left unaddressed when crypto-assets do not qualify as financial instruments. Section II sets out the legal basis of the Advice; Section III sets out the rationale of the Advice; Section IV outlines key concepts and provides an overview of the crypto-asset ecosystem; Section V assesses the risks and issues that regulators should consider when dealing with crypto-assets; Section VI looks at the circumstances under which crypto-assets may qualify as MiFID financial instruments or not; Section VII outlines how the current financial services rules apply to those crypto-assets that qualify as MiFID financial instruments and the challenges that arise as a result; Section VIII outlines ESMA's position on the gaps and issues that EU policymakers should consider, and if relevant and subject to further cost-benefit analysis, seek to address.

11. Considering the novelty of crypto-assets and the evolving business models, ESMA expects that some follow-up work will be needed, as the market develops: i) on how the existing regulatory framework applies to crypto-assets which fall within its scope; and ii) on what requirements could be considered for types of crypto-assets which are currently not subject to any EU rules and how to define the scope of such measures. ESMA will continue actively monitoring market developments, in an effort to foster supervisory convergence among NCAs. ESMA will also continue to engage with global regulators, as we believe international cooperation is required to address this global phenomenon.

II. Legal basis

12. Article 9(4) of its founding Regulation 1095/2010 requires ESMA to establish a Committee on financial innovation "with a view to achieving a coordinated approach to the regulatory and supervisory treatment of new or innovative financial activities and providing advice for the Authority to present to the European Parliament, the Council and the Commission." [5]

13. In late 2017, ESMA identified Initial Coin Offerings (ICOs) and crypto-assets as an issue requiring consideration through its Standing Committee on Financial Innovation. We were aware that the amount of money raised from investors through ICOs was growing quickly. The number and market capitalisation of crypto-assets was developing rapidly as well. We were concerned about the speculation around ICOs and crypto-assets and their high price volatility and the fact that these activities were conducted outside of the regulated space. Some Member States were considering specific regulation to bring them into regulatory scope. Considering the novelty of the phenomenon, the evolving business models and the fact that the existing regulatory framework was not designed with these innovations in mind, we believed it appropriate for ESMA to examine and advise policy makers on the risks and issues raised by ICOs and crypto-assets and the extent to which these are addressed by the existing regulatory regime. ESMA's conclusions are set out in this document, in the form of Advice to the European

[5] Regulation (EU) 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84)

Parliament, the Council and the Commission in accordance with Article 9(4) of its founding regulation.

III. Background

14. In November 2017 and February 2018 respectively, ESMA issued two Statements on Initial Coin Offerings (ICOs) and a joint-Warning on Virtual Currencies (VCs) together with EBA and EIOPA, as we were concerned about the speculation around these instruments and the fact that investors did not appreciate the high risks that they represented. The ICO Statement to firms also reminded firms involved in ICO related activities of their obligations under the EU regulatory framework. In its 2018 FinTech Action plan, the European Commission requested the ESAs to assess the suitability of the current EU regulatory framework with regards to ICOs and crypto-assets more generally.[6]

15. Following these publications, ESMA continued to monitor the development of ICOs and crypto-assets and prepared an assessment of the suitability of the current regulatory framework in relation to these instruments, drawing on a survey to NCAs on the legal qualification of crypto-assets whose outcomes are presented in Annex 1. This work highlighted that while business models are still evolving and it remains unclear how the crypto-asset phenomenon may develop, an entire crypto-asset ecosystem is emerging, e.g., with the development of secondary markets and safekeeping/custody type services for crypto-assets. It also highlighted the wide variety of crypto-assets issued and the many regulatory issues they raise, as the existing rules were not designed with these instruments in mind.

16. ESMA considers that these issues should be drawn to the attention of policymakers so that they could be taken into account in determining whether the current legislative framework is appropriate. In turn, we have used our powers under Article 9 (4) to provide Advice to the European Parliament, the Council and the Commission.

IV. Actors and business models

17. Crypto-assets can be defined as a type of private asset that depends primarily on cryptography and Distributed Ledger Technology as part of their perceived or inherent value.[7] In this report, ESMA uses the term to refer to both so-called virtual currencies and digital tokens issued through ICOs. Also, crypto-asset means an asset that is

[6] European Commission, 2018. 'FinTech Action plan: for a more competitive and innovative European financial sector', March 2018. Available at https://ec.europa.eu/info/publications/180308-action-plan-fintech_en
[7] FSB, 2018. 'Crypto-asset markets, Potential channels for future financial stability implications', Glossary, Oct 2018. Available at http://www.fsb.org/wp-content/uploads/P101018.pdf

neither issued nor guaranteed by a central bank.[8] A glossary of the main terms used in this document is available in Appendix 1.

18. Hundreds of crypto-assets have been issued since Bitcoin was launched in 2009. There are more than 2,050 crypto-assets outstanding representing a total market capitalisation of around EUR 110bn as of end-December 2018 – down from a peak of over EUR 700bn in January 2018.[9] Bitcoin represents just over half of the total reported value of market capitalisation, with the top five crypto-assets representing around 75% of the reported market capitalisation.

19. Crypto-assets may have different features and/or serve different functions. Some crypto-assets, sometimes referred to as 'investment-type' crypto-assets may have some profit rights attached, like equities, equity-like instruments or non-equity instruments. Others, so-called 'utility-type' crypto-assets, provide some 'utility' or consumption rights, e.g., the ability to use them to access or buy some of the services/products that the ecosystem in which they are built aims to offer. Others, so-called 'payment-type' crypto-assets, have no tangible value, except for the expectation they may serve as a means of exchange or payment to pay for goods or services that are external to the ecosystem in which they are built. Also, many have hybrid features or may evolve over time.

Distributed Ledger Technology, private and public keys

20. Distributed Ledger Technology (DLT) is a means of saving information through a distributed ledger, i.e., a repeated digital copy of data available at multiple locations.[10] DLT is built upon public-key cryptography, a cryptographic system that uses pairs of keys: public keys, which are publicly known and essential for identification, and private keys, which are kept secret and are used for authentication and encryption.

21. Crypto-assets are one application of DLT. While all crypto-assets utilise some form of DLT, not all applications of DLT involve crypto-assets. The most common types of crypto-assets at present are those issued on permissionless ledgers.

22. Crypto-assets function using three fundamental pieces of information: the address, and the public and private keys corresponding to that address. The private key is generated first. Then, the corresponding public key is derived from the private key using a known algorithm which varies across protocols.[11] The address, which is associated with a

[8] For example, Central Bank Digital Currencies (CBDC) are not considered in this report. For further details on CBDC see BIS, 2018. 'Committee on Payments and Market Infrastructures, Central bank digital currencies', March 2018. Available at https://www.bis.org/cpmi/publ/d174.pdf

[9] Coinmarketcap, 2018. Figures have been converted into EUR using ECB's exchange rates. Available at https://coinmarketcap.com/all/views/all/

[10] For further information on DLT and its potential benefits and risks when applied to financial securities markets, see ESMA, 2017. 'The Distributed Ledger Technology Applied to Securities Markets', February 2017. Available at https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf

[11] For most crypto assets, including Bitcoin and Ether, the public-key cryptography is based on elliptic curve digital signature algorithms (ECDSAs). Elliptic curve cryptography is said to be superior to the Rivest-Shamir-Adleman (RSA) and Diffie-Hellman (DH) algorithms. Inferring the private key from the public key in this cryptographic system is considered impossible today (no algorithms to solve the discrete logarithms on which elliptic curve cryptography is based have been found yet).

balance and used for sending and receiving assets, is a shorter, representative form of the public key (it is effectively a cryptographic hash of the public key).

23. Practically, the transfer of crypto-asset X from owner A to B works as follows: A generates a transaction that includes A's address, B's address and A's private key (without disclosing what A's private key is). The transaction is broadcast to the entire network, which can verify from A's private key that A has the authority to transfer the crypto-asset on the address it is sending from.

24. The private key is what grants a user the right to dispose of the crypto-assets at a given address. Losing its private key is equivalent to losing the right to move its assets around, hence the need to keep private keys safe.[12] Importantly, what makes the system safe is the impossibility to infer the public key from the address or to infer the private key from the public key. Meanwhile, the entire network can derive the public key from the private key and hence authenticate a given transaction.

Digital wallets

25. Digital crypto-asset wallets are used to store public and private keys and to interact with DLTs to allow users to send and receive crypto-assets and monitor their balances. Crypto-asset wallets come in different forms. Some support multiple crypto-assets/DLTs while others are crypto-asset/DLT specific. There are software/hardware wallets and so-called cold/hot wallets. A software wallet is an application which may be installed locally, e.g., on a computer or mobile phone, in which case it is only accessible from that specific computer or mobile phone. Other software wallets are run in the cloud, meaning that they are accessible from any computing device or location. A hardware wallet is a physical device, like a USB key. Hot wallets are connected to the internet while cold wallets are not. Software wallets are usually hot wallets, while hardware wallets tend to be cold wallets, although there may be some variations.

26. Hot wallets are generally seen as less secure because of their propensity to be hacked. Yet, while crypto-assets in hot wallets may be spent at any time, a cold wallet has to be 'connected' to the internet first. Some hardware wallets provide enhanced security features, e.g., by requiring the user to physically press or touch the wallet in order to sign a transaction.

27. DLT networks typically provide their own wallet functions, e.g., Bitcoin Core for Bitcoin or Mist Browser for Ether.[13] There are also specialized wallet providers. Some wallet providers, so-called custodial wallet providers, not only provide wallets to their clients but also hold their crypto-assets (i.e., their private keys) on their behalf.

[12] Landau, 2018, 'Les crypto-monnaies, rapport au Ministere de l'Economie et des Finances', July 2018. Estimates suggest that a significant portion of bitcoins (maybe 30%) have been lost and now sit idle at an address that Satoshi Nakamotowo is said to own.

[13] Ethereum defines its wallet as 'a gateway to decentralized applications on the Ethereum blockchain. It allows to hold and secure ether and other crypto-assets built on Ethereum, as well as write, deploy and use smart contracts.'

Miners and distributed consensus

28. DLT uses distributed consensus to verify and confirm transactions, and consensus is reached via a network of computers, called miners.[14] Miners effectively provide the necessary computational power to validate transactions and include them in the next block of transactions in the chain.

29. Miners are expected to constantly work on verifying transactions and are incentivized to do so through a fee.[15] The amount of the fee is typically set by the initiator of the transaction depending on the circumstances and what he perceives as the right level to provide for both a timely and cost efficient confirmation of the transaction. While in principle the confirmation is meant to be almost instantaneous, there may be delays in practice, e.g., because of congestion issues, and certain transactions may not be confirmed before several hours or sometimes even days.

30. Mining and consensus set-ups vary across networks. Some DLT networks, e.g., the Bitcoin or Ethereum blockchain, are permissionless, meaning that virtually anyone can become a miner in these networks, although in practise mining is highly concentrated for Bitcoin[16] and Ethereum.[17] Other DLT networks are permission-based, in which case only those parties that meet certain requirements are entitled to participate to the validation and consensus. Consensus mechanisms aim to mitigate the risk of network participants posting false transactions, also known as the Byzantine Fault problem.[18] The way in which consensus is reached may vary. The most prominent consensus mechanisms to date are 'Proof of Work' and 'Proof of Stake'. The Proof of Work[19] consensus, originally used by the Bitcoin blockchain, involves all miners in an extensive 'guessing and checking'-puzzle. It is generally seen as extremely energy intensive and creates scalability issues. Proof of Stake[20] consensus seeks to overcome these issues by reducing the number of network participants working on the verification and validation of new transactions. However, it raises other issues, e.g. few participants may effectively take control of the network.

31. Most of those crypto-assets issued recently, including through ICOs, rely on permissionless DLTs, which raises specific governance and liability issues. However some crypto-assets, including tokenised forms of traditional financial assets, are issued

[14] The terminology and exact role of the network of computers may vary depending on the consensus mechanism. The term 'miners' is typically used for 'Proof-of-Work', while 'forgers' is often used for 'Proof-of-Stake' mechanisms (see below).
[15] In many protocols these incentives are adjusted through time, so that it becomes increasingly difficult to mine the respective crypto-assets. For bitcoin, rewards granted in the form of newly issued bitcoins will decrease to zero after 21,000,000 bitcoins have been mined. Mining after this point will be incentivized by transaction fees paid to miners only.
[16] Blockchain.com, 2018, the six largest miners control c.75% of Bitcoin's hash rate and the biggest miner has a 16% market share. See: https://blockchain.info/pools
[17] Gastracker.io, 2018, the three largest miners controls c.70% of Ether's hash rate and the biggest miner has a 40% market share. See : https://gastracker.io/stats/miners
[18] The 'Byzantine Fault problem' echoes the dilemma of generals agreeing on and verifying a collective military action, while avoiding that the messengers used to communicate are caught and false messages are sent.
[19] 'Proof-of-Work' (PoW) uses 'brute force' and therefore requires high computational power. As Satoshi Nakamoto defines it, 'proof-of-work' is essentially one-CPU-one-vote'. PoW serves to make it difficult to attack the network, by requiring potential attackers to control more than 50% of the CPU of the network.
[20] 'Proof-of-stake' (PoS) requests participants to demonstrate ownership of a pre-defined crypto-asset. With PoS, a person can mine or validate block transactions according to how many coins he or she holds.

and transacted using permissioned DLTs. There may also be hybrid models where a combination of permissioned and permissionless DLTs may be used.

32. Once a new block is verified, all the transactions within it are permanently recorded on the chain and become immutable. However, network participants typically wait until more blocks have been mined to consider the transaction final, due to the risk of concurring chains of blocks. Each party who participates in the validation process has an identical up-to-date copy of the chain or public ledger, which is a record of all the transactions. Each party's copy of the ledger is updated every time a new block is found. After a new block is confirmed, miners start mining the next block. In case of (temporarily) concurring chains of blocks, the longest chain is by default considered the valid one.

Developers and smart contracts

33. Developers work on developing the protocol, including the smart contracts that support DLT networks and crypto-asset activities. Smart contracts are self-executing pieces of code that replicate a given contract's terms. They effectively translate complex contractual terms, e.g., payment terms and conditions, into computational material to automate the execution of contractual obligations. Smart contracts may be used to provide specific guarantees, e.g., for Initial Coin Offerings (ICOs) the guarantee that the funds will be returned to the investor in case the ICO does not reach the minimum subscription target.

Initial Coin Offerings (ICOs)

34. Many crypto-assets have recently been issued through so-called ICOs. ICOs effectively allow businesses to raise capital for their projects, by issuing digital tokens in exchange for fiat currencies or other crypto-assets, e.g., Bitcoin or Ether. ICOs are typically promoted on the web and social media to potential investors using so-called 'white papers'. Some digital platforms have specialised in the promotion of ICOs.

Trading platforms

35. Crypto-assets may be traded or exchanged for fiat currencies or other crypto-assets after issuance on specialised trading platforms. Estimates suggest that there are more than 200 trading platforms operating globally, although a handful concentrate most of the flows.[21,22] The largest platforms are currently located outside of the EU, in Asia or in the United States. Only between a fourth and a third of those crypto-assets issued through ICOs are being traded.[23,24,25] The daily trading volumes are in the range of USD

[21] As an example, Coinmarketcap.com listed 204 platforms as of 7 January 2019. Other estimates go beyond 500 exchanges. See https://news.bitcoin.com/the-number-of-cryptocurrency-exchanges-has-exploded/.
[22] According to Coindesk, State of Blockchain, five platforms control almost the entirety of the trading of Ether
[23] Benedetti & Kostovetzki, 2018. 'Digital Tulips? Returns to investors in Initial Coin Offerings', May 2018.
[24] https://icorating.com/pdf/1/1//mjL8hLbkOfPuJCo2KCKq6gPwZUYd72WZrGMSIeco.pdf
[25] Different elements may explain this low ratio. Issuers typically have to pay a high fee to be listed on a trading platform. Some platforms may impose minimum listing requirements. Also Issuers may impose a lockup period before the crypto-asset may be traded. A number of ICOs have been identified as scams, in which case the issuer may not want to list the crypto-asset.

10-15bn, down from a peak of around USD 70bn in January of 2018.[26] These figures need to be taken with caution though as a number of platforms seemingly inflate the volumes that they trade. Also, while there are over 2,050 crypto-assets, most trading happens in Bitcoin, followed by Tether and Ether.[27]

36. The business models, the range of services offered and the level of sophistication vary across platforms. Some platforms may provide brokers/dealers type services while others are more akin to multilateral trading systems. Some platforms, so-called 'centralised' platforms, hold crypto-assets on behalf of their clients while others, so-called 'decentralised' platforms, do not. Another important distinction between centralised and decentralised platforms is that trade settlement typically occurs on the books of the platforms (off-chain) in the case of centralised platforms, while it occurs on DLT for decentralised platforms (on-chain). Some platforms have adopted good practices from traditional securities venues while others use simple and inexpensive technology. Some incorporate a detailed back-office and administrator application for full user control including Know Your Customer (KYC) and Anti-Money Laundering (AML) functionalities. Others seemingly fail on having the necessary resources and processes in place to address those risks.

37. Trading platforms earn revenues from listing, trading and sometimes safekeeping fees. Listing fees on crypto-asset trading platforms can be significant and range from USD 50,000 to USD 1,000,000.[28] This may create a barrier to entry for smaller issuances and exacerbates the risk of conflict of interest. It is unclear whether platforms routinely undertake due diligence of new crypto-assets. Trading fees also tend to be higher than for traditional securities and may vary depending on the volumes of trades executed by the client and the type of orders.[29] Some platforms, apply a maker/taker model, where only takers, and not makers, have to pay transaction fees.[30]

Investors into crypto-assets

38. Information on the profile of crypto-asset investors is limited. Some estimates suggest however that the investor base has expanded from the original tech-savvy community to a broader audience, including both retail and institutional investors.[31] ICOs do not typically provide for minimum investment amounts nor are they necessarily limited through 'private placement' regimes to professional or more sophisticated investors, meaning that even smaller investors can buy crypto-assets at the issuance stage.

---

[26] Daily consolidated trading volume across all crypto-assets on coinmarketcap.com.
[27] According to Coinmarketcap.com, Bitcoin, Tether and Ether concentrated almost 75% of trading volumes in December 2018.
[28] https://www.businessinsider.nl/cryptocurrency-exchanges-listing-tokens-cost-fees-ico-2018-3/?international=true&r=UK
[29] Some of the largest crypto-asset trading platforms charge fees of 0.3% on average, see: https://www.bloomberg.com/news/articles/2018-03-05/crypto-exchanges-raking-in-billions-emerge-as-kings-of-coins.
[30] Buyers and sellers are referred to as either makers (the users who set a limit price on their orders) or takers (those that match the price and consume available liquidity). Makers usually have their limit orders added to the order book. The order book retains the order until the taker enters a matching order.
[31] As an example, a recent survey in the Netherlands highlighted that there were 490,000 households with crypto investors in the country (out of 7m households in total). The invested amount is generally small, less than EUR 1,000 in 69%. Only 2% invest more than EUR 10,000. In only few cases are these investments made through ICOs (i.e., on the primary market), the vast majority being made through crypto-asset trading platforms (i.e., on the secondary market).

Similarly, there are typically no minimum on the amounts that may be traded on crypto-asset trading platforms.

39. There are more than 28 million digital crypto-asset wallets outstanding, according to some sources.[32] However, this does not mean that there are 28 million investors in crypto-assets as a single investor may use several wallets and many wallets may be inactive. Indeed, some investors may use different wallets for security reasons or because a single wallet is unable to accommodate crypto-assets that use different protocols. Conversely, it is possible that some custodial wallet providers use a single wallet to hold assets on behalf of several clients.

V. Risks and issues for consideration by regulators

40. A consideration for regulators is the wide variety of crypto-assets being issued as they may not all raise the same risks and issues.

41. Another consideration is the need to appreciate the risks not only in relation to the issuance and distribution of crypto-assets but also their trading and their safekeeping, i.e., the whole lifecycle of crypto-assets. This means that a series of parties may be subject to regulation: the issuer of the crypto-assets, the platform where they are distributed and/or transacted, and the provider of custody/safekeeping services.

42. There are also risks that are specific to the underlying technology used, including the fact that it is still a nascent technology and the fact that it is by nature 'distributed'.

Types of crypto-assets

43. Hundreds of crypto-assets have been issued since Bitcoin was launched in 2009 and they can have many different features, as already discussed.

44. While some crypto-assets may fall within the scope of EU financial regulation already, others may not and regulators need to consider whether there is a need to bring them into scope, considering the risks that they may pose to their objectives of investor protection, financial stability and market integrity. Because not all crypto-assets share the same characteristics and purpose, there may be a need to distinguish across them. Also, while certain crypto-assets are outside of the scope of EU financial regulation, they may still be perceived as security-like investments by retail investors, e.g., due to the possibility of trading them on secondary markets.

45. Another consideration is the fact that the frontier between crypto-assets and traditional financial assets is blurring as some traditional financial assets are starting to be issued and transacted on DLT and the business models are evolving.

Risks to investor protection and market integrity

[32] https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/, as of end September 2018.

46. An issue that arises is whether investors understand the risks that they may be exposed to prior to investment and whether they are making investments that are appropriate to their needs.

47. Most businesses raising capital through ICOs are at the initial stages of development, often not even operating businesses but just ideas, even if we are starting to see some larger companies issuing crypto-assets as well. The likelihood that they fail is therefore high and investors have a significant risk to lose their capital. One report of a sample of ICOs from 2017 suggests that a significant minority (30%) have lost all of their value, and a vast majority are valued at below their ICO price. Some projects did, however, have working products or prototypes.[33]

48. Although many crypto-assets may be available for trading on specialised trading platforms after issuance, their liquidity is typically shallow and investors may have a limited possibility of liquidating an investment. The information about the project and the issuer may also be limited considering that they are usually at a very early stage of development. Another issue has to do with the variety of crypto-assets issued and the different rights attached to them, which may not be easily understood by investors, and also the fact that there may be risks that are specific to their underlying technology as discussed below.

49. There have also been widespread reports and concerns around fraudulent ICOs, whereby crypto-assets either do not exist or issuer/developers disappear after the ICO. These could represent up to 80% of ICOs according to some sources.[34]

Risks from secondary trading

50. Many issues pertaining to platforms trading crypto-assets are not in essence different from existing ones applicable to trading venues for traditional securities, even if they may arise in a different way. These include: whether the platform has the necessary resources to effectively conduct its activities and address the risks that may arise from them; whether it has established and maintains adequate arrangements and procedures to ensure fair and orderly trading; whether it has adequate measures to prevent potential conflicts of interest and whether it provides access to its services in an undiscriminating way.

51. Other important issues have to do with price discovery mechanisms and market integrity and include whether pre- and post-trade information made available by the platform is sufficient to support market efficiency, fair and orderly trading and whether the platform has adequate rules, surveillance and enforcement mechanisms to deter potential market abuse. While these issues are not unique to crypto-assets trading platforms they may be exacerbated in the case of crypto-assets because of their high price volatility and often low liquidity. Another important consideration in relation to market integrity is the fact that investors typically access crypto-asset trading platforms directly, without an

[33] EY, 2018. 'ICOs the Class of 2017 – one year later', October 2018. Available at https://www.ey.com/Publication/vwLUAssets/ey-study-ico-research/$FILE/ey-study-ico-research.pdf
[34] https://cryptoslate.com/satis-group-report-78-of-icos-are-scams/

authorised intermediary being involved, which raises the issue of whether the platforms are in the position to and effectively do conduct checks on those clients.

52. There are business continuity issues of the platforms, which again although not unique may be exacerbated in the case of crypto-asset platforms because they are still relatively new and with limited resources. As an example, investors could face difficulties recovering their funds in times of financial distress.

53. In addition, there are other issues that are specific to the business models of crypto trading platforms, such as:

Centralised platforms

54. Centralised platforms typically take control of client crypto-assets (e.g., they hold clients' private keys on their behalf or keep clients' crypto-assets in a single DLT account under the platform's own private key) and may also hold fiat money on their behalf; the issue is therefore whether the platform has the necessary measures in place to segregate and safeguard these assets (crypto and fiat). Noteworthy, several centralised platforms have been hacked in the past, resulting in million losses for their users.

55. On centralised platforms, transaction settlement happens in the books of the platform and is not necessarily recorded on DLT. In those cases (off-chain settlement), confirmation that the transfer of ownership is complete lies with the platform only (no trusted third party involved); investors have therefore a material counterparty risk vis-à-vis the platform, e.g., in case it is malevolent or does not function properly.

Decentralised platforms

56. With decentralised platforms, investors remain in control of their crypto-assets and transaction settlement happens on DLT (on-chain), sometimes using so-called atomic swaps[35] or other forms of smart contracts. While this set-up helps mitigate counterparty risks vis-à-vis the platform, it also has some drawbacks (see below for a discussion of the risks attached to the self-holding of crypto-assets). Decentralised platforms also have the same vulnerabilities/issues as the DLT on which they are built, e.g., there may be delays in the processing of the transactions or governance issues (see below).

57. In addition, decentralised platforms do not typically have the ability to convert fiat into crypto and centralised exchanges are often used as an initial stepping stone to purchase crypto with fiat even for those ultimately planning to trade on decentralised rather than centralised exchanges.

Risks in relation to crypto-assets custody/safekeeping

[35] By using atomic swaps the exchange of the two crypto-assets resulting from a trade will initially be locked and can only be retrieved by the relevant counterparty using a cryptographic hash function. Thereby, a time-lock function ensures the refund of the two crypto-assets to the original counterparty in the case that one of the counterparties did not retrieve the crypto-asset within a predefined time period.

58. Investors may choose to hold their crypto-assets themselves, i.e., they remain in full control of their private keys, using hardware or software wallets. The main advantage of this approach is that the investor remains the sole owner of its private keys at all times, which reduces the risk of a hack, as there is no central point of failure. Yet, not all investors may have the necessary expertise and equipment to safe keep their private key properly. Also this model may be ill-suited to certain types of investors, e.g., institutional investors, where several individuals and not just one need to have control of crypto-assets.

59. Other investors entrust the custody of their crypto-assets to custodial wallet providers, which hold crypto-assets (e.g., the private keys) as an agent on behalf of the investor and has at least some control over these crypto-assets. The issue is therefore whether the custodial wallet providers have the necessary measures in place to segregate and safeguard these assets.

60. Of note, there is often no clear separation of duties and many crypto-asset trading platforms may act as custodial wallet providers as highlighted above.

Other risks stemming from the underlying technology

61. Although DLT may provide a number of potential benefits, it also raises a number of specific risks and issues, as highlighted in ESMA DLT report.[36]

62. First, there may be flaws in relation to the technology itself, e.g., in the protocols or the smart contracts that come on top. While DLT supporters generally see DLT as more secure than many existing systems, it may still be possible to tamper with the records or the technology may not always function properly, e.g., during peaks of activity. Also, the smart contracts may not work as intended, e.g., in case of coding errors.

63. More generally, crypto-assets may raise specific technology and cyber security risks, because of their very nature and also the fact that DLT is still a nascent technology and largely untested in financial markets. Also, the fact that few people have the necessary skillset to understand the intricacies of the technology may exacerbate operational risks and the risk of fraud. As an example, cases have been reported of ICO issuers diverting contributions of investors from supposedly secured DLT accounts or smart contracts.

64. Second, there are issues around governance, privacy and territoriality that are attached to the distributed nature of DLT. The distributed and cross-border nature of the technology may create specific jurisdictional issues for regulators. Importantly, while these issues may be mitigated in the case of permission-based DLTs through specific arrangements, they are typically exacerbated in the case of permissionless DLTs.

65. The distributed nature of DLT, including the use of consensus to validate transactions and the use of self-executing pieces of codes, implies that establishing clear responsibilities and liabilities, e.g., in case of errors or malevolent activities, may be a

[36] ESMA, 2017, 'The Distributed Ledger Technology applied to securities markets', Feb 2017. Available at https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf

challenge in the absence of clear rules established at the outset. Another related issue that is particularly relevant to permissionless DLTs has to do with the role of miners, as they provide the necessary 'fuel' to verify and make transactions final. Unless they receive the proper incentive to continuously mine transactions, they may suspend their activities, in which case transactions would be left pending. Meanwhile, the concentration of mining activities in a few hands may raise pricing and competition issues. There is also the risk of forks[37] which could split away market participants, increase the number of crypto-assets or make some crypto-assets obsolete.

66. The distributed nature of DLT also implies some form of publicity, namely that all participants share the same records, which if not handled carefully, could raise privacy issues, e.g., in relation to client data. There is also the risks that some participants misuse the information that may be available to them, e.g., to front run transactions of others, unless proper safeguards are in place.

67. Also in the absence of adequate controls, because of the anonymity attached to private/public keys, crypto-assets may be prone to the risk of fraud or other illicit activities, including money laundering.

Risk to financial stability

68. At this point, we do not believe that crypto-assets represent a threat to financial stability, considering the relatively small volumes involved and the limited linkages with traditional financial markets.[38] Despite the recent hype around ICOs, crypto-assets are still relatively small compared to the global financial system: the total market capitalisation of crypto-asset is around USD 130 billion to be compared with USD 22 trillion for the S&P500 market capitalisation as of end-December 2018 for example.

69. Most investment in crypto-assets seems to come from savings, rather than leverage, and there does not appear to be widespread liquidity mismatch or maturity transformation. However, there are some anecdotal indications of leveraged purchases by investors and we believe that it is important to monitor the potential macro financial risks that may stem from crypto-assets.

Potential benefits of ICOs and crypto-assets

70. Provided the relevant safeguards are in place, ICOs could provide a useful alternative funding source for blockchain start-ups and other innovative businesses that would find it difficult or costly to raise capital through traditional funding channels. They could also provide a fast and effective means to raise money from a diverse investor base.

---

[37] A fork is a change to the DLT protocol. A hard fork is defined as a change that requires all nodes or users to upgrade to the latest version of the protocol software, or creates two versions of the protocol going forward. FSB, 2018, 'Crypto-asset markets: Potential channels for future financial stability implications'. October 2018. Available at: http://www.fsb.org/wp-content/uploads/P101018.pdf

[38] See for example FSB, 'Crypto-asset markets, Potential channels for future financial stability implications', Oct 2018. Available at http://www.fsb.org/wp-content/uploads/P101018.pdf

71. ICOs could represent an attractive, although risky, investment opportunity, including for smaller investors that do not typically get access to early-stage financing investments.

72. More generally, we see the so-called 'tokenisation' of assets as a potential long term trend that has the potential to create beneficial outcomes for both market participants and investors. Tokenisation is a method that converts rights to an asset into a digital token. It is effectively a means to represent ownership of assets on DLT. Virtually anything can be tokenised, ranging from physical goods to traditional financial instruments. Some NCAs have provided examples of live cases where a firm has issued a traditional investment in a tokenised form, which was achieved faster and at lower cost than a traditional issuance process.

73. Tokenisation has the potential to enhance the liquidity of certain financial assets, e.g., unlisted shares or syndicated loans, by making transfer of ownership easier and faster. It may also reduce the need for intermediaries. In addition, DLT also facilitates the use of smart contracts, which automate the execution of contract obligations, thereby potentially reducing risks and costs. This could in turn provide positive outcomes for both market participants and end-consumers.

74. We anticipate potential opportunity costs if these developments were unduly restricted.

Need for legal certainty

75. Another issue has to do with the uncertainty that currently prevails around the legal treatment of crypto-assets and the way in which the existing EU regulatory framework may apply to them. This uncertainty creates risks to investor protection and does not allow for the development of a sustainable ecosystem.

VI. Legal qualification of crypto-assets

76. This section discusses the legal qualification of crypto-assets under EU financial securities laws, in line with ESMA's remit. See the EBA's report and advice on crypto-assets for a discussion of the qualification of crypto-assets under the second Electronic Money Directive (Directive 2009/110/EC) and the second Payment Services Directive (Directive 2015/2366/EU).[39]

77. There is currently no legal definition of 'crypto-assets' in the EU financial securities laws.[40] A key consideration of the legal qualification of crypto-assets is whether they may qualify as MiFID II financial instruments. The existing EU financial regulation establishes a comprehensive regulatory regime governing the execution of transactions in financial instruments.

---

[39] See footnote 3

[40] However, note that Directive 2018/843 of the European Parliament and Council of 30 May 2018 amending the Anti-Money Laundering Directive (EU) 2015/849 includes a definition of "virtual currencies" as " "*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*"

78. “Financial instruments” are defined in Article 4(1)(15) of MiFID II as those “instruments specified in Section C of Annex I.” These are *inter alia* ‘transferable securities’, ‘money market instruments’, ‘units in collective investment undertakings’ and various derivative instruments.

79. “Transferable securities” under Article 4(1)(44) of MiFID II, means those “classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:

- shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
- bonds or other forms of securitised debt, including depositary receipts in respect of such securities;
- 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, currencies, interest rates or yields, commodities or other indices or measures;”.

80. In an effort to determine the legal status of crypto-assets and determine possible applicability of EU financial regulation ESMA undertook a survey of NCAs in the summer of 2018 with the aim to collect detailed feedback on the possible legal qualification of crypto-assets as financial instruments. The survey questions were designed to determine the way in which a given Member State had transposed MiFID II into its national law and, based on that transposition, whether a sample set of six crypto-assets issued in an ICO qualified as ‘financial instruments’ under their respective national laws. The sample crypto-assets were real crypto-assets that may be available to European investors. They reflected differing characteristics that ranged from investment-type (crypto-asset cases 1 and 2), to utility-type (case 5), and hybrids of investment-type, utility-type and payment-type crypto-assets (cases 3, 4 and 6). Pure payment-type crypto-assets were not included in the sample set on purpose as they are unlikely to qualify as financial instruments. The following is a summary of the survey sample results as reflected in the majority of the responses. The detailed survey results together with the features of the six sample crypto-assets are provided in Annex 1.

81. Noteworthy, the results reflected below should not be extrapolated to the entire crypto-asset universe. In particular, payment-type crypto-assets, like the Bitcoin which accounts for around half of the total market value of crypto-assets, are not represented in the survey sample. Also, the actual classification of a crypto-asset as a financial instrument is the responsibility of an individual NCA and will depend on the specific national implementation of EU law and the information and evidence provided to that NCA.

82. The survey highlighted that most NCAs assessed that crypto-asset case 1, 2, 4 and 6 could be deemed as transferable securities and/or other types of financial instruments as defined under MiFID II, although there were some variations across NCAs on the number of cases that would qualify, depending on the Member State’s national definition

of financial instruments. This effectively suggests that a number of crypto-assets (our estimates suggest that crypto-assets that bear resemblance with cases 1, 2, 4 and 6 might represent 10 to 30% of the total in number, although these figures need to be considered with caution, as data on crypto-assets are patchy and the market constantly evolving), provided they meet the relevant conditions, may qualify as transferable securities and/or other types of financial instruments. These crypto-assets should therefore comply with the existing EU financial regulation (whose application depends on the qualification as financial instrument under MiFID II), which in turn raises the issue of the potential gaps and issues that may exist in the current rules when it comes to supervising those instruments.

83. Indeed, there was broad agreement among NCAs that the crypto-assets that meet the necessary conditions to qualify as a financial instruments should be regulated as such. At the same time, a number of NCAs suggested that changes to existing legislation or additional provisions may be needed to respond to the unique characteristics of the sector, e.g. the decentralized nature of underlying technology, risk of forks, and the custody of the underlying assets. NCAs also highlighted that a review of existing provisions related to clearing, settlement, safekeeping and record of ownership may be necessary.

84. This view is also supported by the fact that ten NCAs have highlighted in their response at least one example of crypto-assets in their jurisdiction (beyond the six crypto-asset cases presented) that would qualify as a transferable security or other type of MiFID II financial instrument.

85. The existence of attached profit rights, without having necessarily ownership or governance rights attached (crypto-asset case 1 and 2), was considered sufficient for a majority of NCAs to qualify crypto-assets as transferable securities (where such crypto-assets also meet the other conditions to qualify as transferable securities), whether as shares or another type of transferable securities not explicitly listed in Annex C of MiFID II. Those NCAs that disagreed with this view may do so on the basis of a more restrictive transposition of MiFID, e.g. a restrictive list of examples of transferable securities. The responses for crypto-asset case 4 suggested that the financial instrument features may prevail for hybrid types of crypto-assets, although views could vary depending on the exact circumstances (see crypto-asset case 3).

86. The fact that no NCA labelled case 5 as a transferable security and/or financial instrument suggests that pure utility-type crypto-assets may fall outside of the existing financial regulation across Member States. The rights that they convey seem to be too far away from the financial and monetary structure of a transferable security and/or a financial instrument.

87. The vast majority of NCAs did not believe that any national rules in place would capture any of the six case studies. However, two NCAs have domestic categories of financial / investment products that are broader than MiFID financial instruments, addressing products that are deemed to have an investment purpose or expectation of returns. For one NCA, this was sufficiently broad to capture five of the six cases. Another NCA has a separate ‘unit of account’ category, potentially catching two cases (1, 4). One NCA is

implementing a bespoke national regime for crypto-assets, which could apply to cases 1 and 3.

88. Noteworthy, the vast majority of respondents considered that the qualification of all crypto-assets as financial instruments has unwanted collateral effects, meaning that there may be a need to distinguish between the different types of crypto-assets. This is understandable considering the variety of crypto-assets being issued. Among the reasons given were 1) the existing regulation was not drafted having these instruments in mind; 2) acknowledging them as financial instruments would grant them potentially unwanted legitimacy; 3) the needed supervisory tools and resources may not be in place.

89. The vast majority of NCAs agreed that all crypto-assets should be subject to some form of regulation. There was little consensus as to whether a bespoke regulatory regime for those crypto-assets that do not qualify as financial instruments should be designed within the scope of MiFID or outside of it. There were as well diverging views regarding the extent of that regulatory regime, although with a broad consensus on that at minimum all activities involving crypto-assets should be subject to anti-money laundering laws (on which see further the EBA's report and advice on crypto-assets[41]).

VII. Regulatory implications when a crypto-asset qualifies as a financial instrument

90. There are a range of approaches to crypto-asset related activities (see section IV on Actors and business models above), and the model chosen will have an impact on which legislation is applicable, and in which way. This section of the Advice summarises a range of legal provisions potentially applicable to crypto-assets when they do qualify as financial instruments. It has not been formulated for any other purpose and should not be relied on to provide a complete statement of the requirements arising under the legislation discussed.

VII.1 The Prospectus Directive

91. The Prospectus Directive[42] (PD) requires publication of a prospectus before the offer of securities to the public or the admission to trading of such securities on a regulated market situated or operating within a Member State, unless certain exclusions or exemptions apply. In particular, the PD specifies that the prospectus shall contain the necessary information which is material to an investor for making an informed assessment of the financial condition of the issuer and of any guarantor, the rights attaching to the securities and the reasons for the issuance and its impact on the issuer. The information shall be written and presented in an easily analysable and comprehensible form. The Prospectus Regulation[43] (PR), which will apply from 21 July

[41] See footnote 3
[42] Directive 2003/71/EC as amended
[43] Regulation (EU) 2017/1129

2019, imposes similar requirements in relation to the public offer of securities to the public.

92. The PD (and the PR) does not directly specify who should draw up the prospectus but requires that the party responsible for the information (being at least the issuer / offeror / party seeking admission to trading / guarantor) is specified in the prospectus. The prospectus cannot be published until it has been approved by the competent authority.

Scope and exemptions

93. The prospectus rules apply only where instruments are transferable securities, as defined in point (44) of article 4(1) of MiFID II. If the instrument does not qualify as a transferable security, any transparency requirements would depend on national law.

94. The size of the offer may not trigger the requirement for the publication of a prospectus:

- Offers below EUR1m are exempt from the obligation to publish a prospectus (EUR1m calculated over 12 months).
- Member States may decide to exempt offers below EUR8m (EUR8m calculated over 12 months) from the requirement to publish a prospectus prepared in accordance with the PR [Art 3.2(b) of the PR which applies from 21 July 2018].
- Between EUR1m and EUR8m, Member States will select a threshold (not higher than EUR8m) under which national requirements apply. National requirements vary by Member State.

95. Offers would also be exempt from the obligation if:

- The offer is addressed only to 'qualified investors', which are essentially professional clients under MiFID II [PD Art 3.2(a)]; or
- The offer is addressed to fewer than 150 natural or legal persons per Member State other than 'qualified investors' [PD Art 3.2(b)]; or
- Investors acquire securities for a total consideration of at least EUR100 000 per investor, for each separate offer [PD Art 3.2(c)];
- The denomination per unit amounts to at least EUR100 000 [PD Art 3.2(d)]; or
- The total consideration in the Union is less than EUR100 000 which shall be calculated over a period of 12 months [PD Art 3.2(e)[44]].

Applicability to crypto-assets

[44] Exemption that applies until the application of the PR (21 July 2019).

96. The prospectus rules should apply to crypto-assets offered to the public, including through ICO, where the instruments qualify as transferable securities. It will therefore not apply to those crypto-assets that do not qualify as transferable securities, in which case disclosure requirements will depend on national law.

97. Provided the issued crypto-assets qualify as transferable securities, a number of ICOs and/or offers may trigger the application of prospectus rules due to their size (i.e., above the threshold that is set in national legislation between EUR1m and EUR8m). Others may fall under the threshold, in which case disclosure requirements will depend on national law again (i.e. below EUR1m, Member States may choose to apply disclosure requirements but not extend the obligation to publish a prospectus; between EUR 1m and EUR 8m they can extend the obligation to publish a prospectus).

98. When it applies, PD (and PR) provides that the prospectus should contain the necessary information which is material to an investor for making an informed assessment of the financial condition of the issuer, the rights attached to the securities and the reasons for the issuance and its impact on the issuer. In the case of crypto-assets, this would likely include detailed information on the issuer's venture, the features and rights attached to the crypto-assets being issued, the terms and conditions and expected timetable of the offer, the use of the proceeds of the offer and the specific risks related to the underlying technology.

99. There are no specific schedules for ICOs/crypto-assets. However, NCAs would use the existing schedules and where necessary require adapted information depending on the specific circumstances of the issuer and the characteristics of the securities. For example, if an ICO takes place and the transaction were to be considered similar in substance to a conventional IPO, the issuer would most likely be required to draft information about itself as though it were an issuer of equity securities.

100. If the crypto-assets are considered akin to equity securities, then a similar logic of using information requirements set out in the equity securities note would apply. The concept of seeking 'adapted' information provides reasonable scope for flexibility in terms of framing a transaction in a way which best reflects an existing construct that is known to the market.

VII.2 The Transparency Directive

101. The Transparency Directive[45] (TD) aims to provide the disclosure of accurate, comprehensive and timely information about issuers whose securities are admitted to trading on a regulated market situated or operating within a Member State. In particular, it requires disclosure of periodic and ongoing information about these issuers, e.g., annual financial reports, half-yearly reports, interim management statements, acquisition or disposal of major holdings and any changes in the rights of holders of

[45] Directive 2013/50/EU amending Directive 2004/109/EC

securities. TD applies only were instruments are transferable securities, as defined in point (44) of article 4(1) of MiFID II.

102. Where the crypto-assets are transferable securities admitted to trading on a regulated market situated or operating within a Member State, their issuers will therefore need to comply with the periodic and ongoing disclosure requirements set in the Transparency Directive.

VII.3 The Markets in Financial Instruments Directive framework

103. The Market in Financial Instruments Directive framework (MiFID II) consist of a directive[46] (MiFID 2), a regulation[47] (MiFIR) and their implementing acts. A firm that provides investment services/activities in relation to financial instruments as defined by MiFID II needs to be authorised as an investment firm and comply with MiFID II requirements. Where crypto-assets qualify as financial instruments, a number of crypto-asset related activities are likely to qualify as investment services/activities such as placing, dealing on own account, operating an MTF or OTF or providing investment advice. The organisational requirements, the conduct of business rules and the transparency and reporting requirements laid down in MiFID II would then apply, depending in some cases on the type of services offered and the type of financial instrument involved.

104. In this section of the Advice, our focus is on the applicability of MiFID II to platforms trading crypto-assets, as they represent the most common type of intermediaries in the space at this point and raise specific risks as discussed above. This is not to say though that other types of crypto-asset intermediaries are non-existent. Again, where crypto-assets qualify as financial instruments, those intermediaries are likely to provide investment services and should therefore be required to comply with applicable MiFID II requirements.

105. A question that arises in relation to platforms trading crypto-asset is the type of MiFID II services/activities that they may provide, as the applicable requirements may vary depending on the services/activities, and sometimes also the type of MiFID financial instrument involved. We have identified three broad categories of platforms at this stage, namely (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. More details on the business models of these platforms is provided in Appendix 2. Noteworthy, a number of platforms may provide different types of services/activities and therefore cut across the three categories above. There are also so-called centralised and decentralised business models as already discussed. Centralised platforms represent by far the bulk of the volumes traded today. However, some hybrid business models, e.g., where the matching of the orders is provided at the platform level (off-chain) but the settlement is

[46] Directive 2014/65/EU
[47] Regulation (EU) No 600/2014

processed on chain have started to emerge. Our current understanding is that fully decentralised platforms are still in their infancy.

106. ESMA's preliminary view is that where crypto-assets qualify as financial instruments, platforms trading crypto-assets with a central order book and/or matching orders under other trading models are likely to qualify as multilateral systems and should therefore either operate under Title III of MiFID 2 as Regulated Markets (RMs) or under Title II of MiFID 2 as Multilateral Trading Facilities (MTFs) or Organised Trading Facilities (OTFs). RMs are operated or managed by a market operator. MTFs and OTFs are operated by a market operator or an investment firm.

107. Where the operators of those platforms are dealing on own account and executing client orders against their proprietary capital, they would not qualify as multilateral trading venues but rather as broker/dealers providing the MiFID II services of dealing on own account and/or the execution of client orders and should therefore comply with the requirements set out in Title II of MiFID 2.

108. Platforms that are used to advertise buying and selling interests and where there is no genuine trade execution or arranging taking place may be considered as bulletin boards and fall outside of MiFID II scope, as per recital 8 of MiFIR.

109. We provide below an overview of the requirements likely to apply to these platforms and their operators. Please note that this overview is not meant to be exhaustive but rather to highlight some of the key requirements that may apply and the issues that they may raise.

VII.3.1 Overview of key requirements likely to apply

Capital requirements

110. Investment firms need to comply with minimum capital requirements as set out in Article 15 of MiFID and Directive 2013/36/EU and Regulation (EU) No 575/2013 (also known as "CRD IV/CRR"). They vary depending on the type of MiFID services/activities, as outlined in Appendix 3. In particular, investment firms operating an MTF or an OTF or dealing on own account need to have an initial capital of EUR 730,000 minimum. Regulated markets need to have available at the time of authorisation and on an ongoing basis, sufficient financial resources to facilitate its orderly functioning, having regard to the transactions concluded on the market and the risks to which it is exposed under Article 47(f) of MiFID.

Organisational requirements

111. Article 16 of MiFID 2 sets out the organisational requirements for investment firms. In particular, Article 16 provides that investment firms should have adequate policies and procedures to ensure compliance with their obligations under MiFID, including in relation to the prevention of conflicts of interest, the approval and distribution of financial instruments to clients, business continuity, integrity and security of data, recordkeeping, internal controls and risk management (see Appendix 4). Noteworthy,

some of these requirements apply to the investment firm in its relationship with its clients and are therefore not relevant when the investment firm operating a trading venue does not have a client relationship with the participant of the trading venue, e.g., an investment firm operating an MTF.

112. Under Article 18, MTFs and OTFs specifically need to : establish transparent rules and procedures for fair and orderly trading and objective criteria for the efficient execution of orders ; have sound management of the technical operations of the facility, including effective contingency arrangements; have transparent criteria to determine the financial instruments that can be traded under their systems; provide, or are satisfied that there is access to, sufficient publicly available information to enable their users to form an investment judgement ; have arrangements to identify and manage potential conflicts of interest ; inform their members on settlement responsibilities and have the necessary arrangements to facilitate efficient settlement of the transactions concluded on their platforms.

113. Article 19 contains specific requirements for MTFs regarding the establishment of non-discretionary rules for the execution of orders in the system. Article 19(5) provides that MTFs cannot execute client orders against proprietary capital or engage in matched principal trading. The specific requirements for OTFs are contained in Article 20 of MiFID 2 (use of discretion, when they can engage in matched principal or dealing on own account, which facilities can belong to the same legal entity, etc.).

114. RMs need to comply with the organisational requirements set out in Article 47(1) of MiFID 2. Article 47(2) provides that RMs, like MTFs, cannot execute client orders against proprietary capital or engage in matched principal trading. RMs also have to comply with specific requirements related to the admission of financial instruments to trading [Article 51 of MiFID 2] and the suspension and removal of financial instruments from trading [Article 52 of MiFID 2].

115. RMs, MTFs and OTFs need to comply with Article 48 which establishes systems resilience, circuit breakers and electronic trading, and Article 49 on tick sizes.

116. To support market transparency and integrity, Article 31 provides that MTFs and OTFs should establish and maintain effective arrangements and procedures to monitor compliance by their members or participants or users with their rules. This includes the monitoring of orders sent, including cancellations and the transactions undertaken by their members or participants or users. MTFs and OTFs should inform immediately their competent authority of any infringements of those rules. Similar or enhanced requirements apply to RMs under Article 54.

117. MTFs operating as SME growth markets need to comply with Article 33 of MiFID 2 (50% of SME issuers, appropriate criteria for initial and ongoing admission, sufficient information upon initial admission, appropriate ongoing reporting, regulatory information on the issuer stored and disseminated to the public, effective systems and controls to prevent and detect market abuse).

Investor protection provisions

118. Investment firms need to fulfil the operations conditions provisions set out in Title II Chapter II of MiFID 2, some of them applying only to the investment firm in its relationship with its clients. These include provisions to identify and to prevent or manage conflicts of interest, provisions to act honestly, fairly and professionally in accordance with the best interest of its clients, provisions to ensure that all information addressed to clients is fair, clear and not misleading and the obligation to execute orders on terms most favourable to the client.

Access to MTFs, OTFs and RMs

119. MTFs and OTFs need to have in place transparent and non-discriminatory rules for access to their facilities according to Article 18(3). Similar provisions apply to RMs under Article 53.

120. In addition, Article 53(3) determines the conditions for RMs and MTFs [see Article 19] to admit members or participants that are not investment firms or credit institutions authorised under Directive 2013/63/EU. Such members or participants must be of sufficient good repute, have sufficient level of trading ability, competence and experience, have adequate organizational arrangements and have sufficient resources for the role to be performed.

121. Under 53(7) the market operator needs to communicate on a regular basis the list of its members or participants of its regulated market to its competent authority.

Pre and post-trade transparency

122. MiFIR sets out transparency requirements for trading venues in relation to both equity and non-equity instruments. For equity instruments, it establishes pre-trade transparency [Article 3], waivers from that pre-trade transparency [Article 4], and restrictions to the use of some of those waivers [Article 5 on Double Volume Cap], post trade transparency [Article 6] and deferred publication [Article 7]. The same structure is replicated for non-equity instruments: pre-trade transparency [Article 8], waivers [Article 9], post-trade transparency [Article 10], and deferred publication [Article 11].

123. Pre-trade and post-trade data should be made available to the public separately and on a reasonable commercial basis and free of charge after 15 minutes [Article 12 and 13 of MiFIR].

Transaction reporting and obligations to maintain records

124. There is an obligation for investment firms to maintain records for five years of the orders in financial instruments as set out in Article 25(1) of MiFIR. A similar requirement applies to operators of trading venues for at least five years as set out in Article 25(2) of MiFIR.

125. Article 26 sets out the obligation for investment firms to report transactions to their competent authority and the details to be reported. The operator of the trading venue is responsible for reporting the details of the transactions where the participant is not an investment firm.

126. Trading venues shall provide competent authorities with identifying reference data in accordance with Article 27 for the purposes of transaction reporting under Article 26 of MiFIR (obligation to supply reference data).

VII.3.2 Possible gaps and issues

127. This sub-Section addresses gaps and issues that arise as a result of the application of MIFID 2/MIFIR legislation to crypto-assets that qualify as a financial instrument. A first issue has to do with the disintermediated access to crypto-asset trading platforms. In case the platform qualifies as RM or MTF, it would need to check that its members or participants are of sufficient good repute, with sufficient level of trading ability, competence and experience and with adequate organizational arrangements and resources. Conducting those checks may be time and resource intensive for the platforms in the case of individual investors, because of their large number, and many individual investors may not pass those tests.

128. The existing pre and post-trade transparency provisions under MiFIR have been designed for respectively equity and non-equity instruments. Our current understanding based on our survey is that, although certain crypto-assets may qualify as MiFID transferable securities, not all jurisdictions may categorise these crypto-assets as equity or non-equity instruments. Transparency requirements may therefore not apply consistently across Member States.

129. The Regulatory Technical Standards relative to various data reporting and record keeping requirements (e.g., transaction reporting, instrument reference data, transparency and DVC data, orderbook data, etc.) will likely need to be revisited, as they were designed to capture traditional instruments and not crypto-assets. Also, the currently used identifiers and classifications (e.g. ISO 6166 ISIN code, ISO 10962 CFI code, and ISO 4217 currency code) have not yet been adapted to the new developments in the crypto-assets domain. This implies that the existing reporting systems will need to be adapted and the respective market participants will need to develop capacity to comply with comprehensive data reporting requirements.

130. Where the trading platforms use decentralised business models, the lack of a clearly identified operator and the reliance on self-executing pieces of code would raise specific issues that would need to be addressed. Meanwhile, decentralised business models might help mitigate some of the risks found in traditional trading venues, e.g., counterparty risk. Our current understanding is that decentralised platforms are still at a nascent stage although they may become more widespread in the future.

131. Also, there may be a need for EU policymakers to clarify the type of investment services/activities that hybrid platforms may provide and hence the rules that may apply to them. Indeed, some hybrid platforms seemingly provide for the matching of orders but not their execution itself, which may be processed through smart contracts. A question that could therefore arise at supervisors is whether these platforms would qualify as RMs, MTFs, OTFs, investment firms or not.

VII.4 The Market Abuse and Short-Selling Regulation

132. The Market Abuse Regulation (MAR)[48] prohibits insider dealing, the unlawful disclosure of inside information and market manipulation (market abuse) in relation to the following instruments: (a) financial instruments admitted to trading on a regulated market or for which a request for admission to trading on a regulated market has been made; (b) financial instruments traded on an MTF, admitted to trading on an MTF or for which a request for admission to trading on an MTF has been made; (c) financial instruments traded on an OTF; and (d) financial instruments not covered by point (a), (b) or (c), the price or value of which depends on or has an effect on the price or value of a financial instrument referred to in those points' [Article 2]. The above prohibitions apply to any person [Article 14].

133. Where crypto-assets qualify as financial instruments, and provided they are traded or admitted to trading on a trading venue (or, where they are not traded on a trading venue, their price or value depends or has an effect on the price or value of a financial instrument traded on a trading venue), MAR would become applicable. In addition, the trading platforms would need to have in place effective arrangements, systems and procedures aimed at preventing, detecting and reporting market abuse [Article 16]. Issuers would need to disclose inside information as soon as possible [Article 17] and to maintain an insider list [Article 18]. Managers at issuers would need to notify the competent authority of every transaction conducted on their own account [Article 19]. Persons who produce or disseminate investment recommendations would also need to ensure that such information is objectively presented [Article 20], which may be particularly pertinent for crypto-asset markets where limited trading volumes and / or concentrated ownership of certain crypto-assets may raise greater risks of conflicts of interest.

134. ESMA has not analysed at this point in time whether the price of a financial instrument could be influenced through manipulative trading activity in crypto-assets that do not qualify as a financial instrument (for instance where the same issuer has issued financial instruments traded on a trading venue and crypto-assets), and whether the current regulatory framework would adequately address that situation. ESMA recommends that this possibility could be considered and addressed in any further MAR revision.

135. Also, the novel nature of crypto-asset market could mean that some new abusive behaviours may arise which are not directly captured by MAR or current market monitoring arrangements. For example, new actors may hold new forms of inside information, such as miners and wallet providers, which could potentially be used to manipulate the trading and settlement of crypto-assets.

[48] Regulation (EU) No 596/2014

136. The application of MAR might also raise specific issues in the case of decentralised trading platforms, as there may be a lack of clarity as to the identity of the market operator.

137. It is noted that where crypto-assets do not qualify as financial instruments, trading activity in them would in principle be out of the scope of MAR.

138. As far as short-selling is concerned, where crypto-assets qualify as financial instruments, they would fall under the scope of the Short Selling Regulation[49] in case a position in the crypto-asset would confer a financial advantage in the event of a decrease in the price or value of a share or sovereign debt (Article 3 of the Short Selling Regulation and Articles 6(2) and 8(2) of Commission Delegated Regulation (EU) 918/2012).

139. However, it is noted that the determination of net short positions for the application of the Short-Selling Regulation is dependent on the list of financial instruments in Annex I of Commission Delegated Regulation (EU) 918/2012). It might be necessary to revise such list to ensure that those crypto-assets (within the scope of financial instruments) that might generate a net short position on a share or on a sovereign debt are explicitly included in that list.

140. ESMA has not analysed whether a transaction in a crypto-asset that does not qualify as a financial instrument could confer a financial advantage in the event of a decrease in the price or value of a share or sovereign debt, and therefore, whether it might be convenient to revise the Short Selling Regulation in this respect.

VII.5 The Settlement Finality Directive and the Central Securities Depositories Regulation

141. These pieces of legislation apply to settlement activities. The Settlement Finality Directive (SFD)[50] aims at reducing systemic risk associated with participation in payment, clearing and securities settlement systems, in particular the risks linked to insolvency of a participant in such a system. SFD applies to systems duly notified as well as any participant in such a system, and to collateral security provided in connection with the participation in a system, or operations of the central banks of the Member States in their functions as central banks.

142. The aim of the Central Securities Depositories Regulation (CSDR)[51] is to harmonize certain aspects of the settlement cycle, settlement discipline and provide a set of common requirements for CSDs operating securities settlement systems in order to enhance cross border settlement in the EU. It applies to the activities of CSDs and to

[49] Regulation (EU) No 236/2012
[50] Directive 2009/44/EC
[51] Regulation (EU) No 909/2014

the settlement of transactions in all MiFID financial instruments, unless specified otherwise.

143. We highlight below some of key requirements provided by SFD and CSDR that may apply to crypto-assets and those parties involved in crypto-asset settlement activities when crypto-assets qualify as financial instruments. Again, please note that this overview is not meant to be exhaustive but rather to highlight some of the key issues that the application of SFD and CSDR to crypto-assets may raise.

VII.5.1 Settlement provisions

144. Different requirements may apply to firms/participants that engage in securities settlement activities, depending on the existence of a 'securities settlement system' and on the applicability of SFD and CSDR.

145. Article 2(a) of SFD specifies that a 'system' shall mean a formal arrangement between three or more participants, with common rules and standardised arrangements for the clearing or execution of transfer orders designated as a system by the Member State whose law is applicable. A system under the SFD is governed by the law of a Member State chosen by its participants (the participants may only choose the law of a Member State in which at least one of them has its head office). Article 2(10) of CSDR further specifies that a 'securities settlement system' means a 'system', as defined in the SFD, that is not operated by a central counterparty whose activity consists of the execution of transfer orders.

146. Criteria typically considered by Member States to designate a securities settlement system under SFD may include the volume and value of all securities transactions that are settled through the system and its systemic importance.

Key provisions, potential gaps and issues, where there is a securities settlement system

147. If there were a 'securities settlement system' for those crypto-assets that qualify as financial instruments, e.g., if the trading platform or the DLT network on which the execution of crypto-asset transactions is concluded were to qualify as such, this system would need to be operated by a 'system operator', which, according to the SFD, means the entity or entities legally responsible for the operation of a system. A first issue that would arise is whether a market operator could be identified, e.g., in case of trading platforms using so-called 'decentralised' business models.

148. If the crypto-assets are transferable securities referred to in Article 3 of CSDR, which are traded on a trading venue or transferred following a financial collateral arrangement, they would have to be recorded with an authorised CSD as defined under Article 2(1)(1) of CSDR. The operator of the trading platform or the DLT network would therefore need to seek authorisation as a CSD (whether the operator should be authorised as trading venue and CSD would require further consideration in that respect) or work with an authorised CSD, which would bear a number of implications in terms of organization, resources and costs. CSDs need to operate under Title III of CSDR. Whether permissionless DLTs, due to the specific governance issues that they

raise, might fulfil these requirements is an issue that requires additional consideration. For example, one issue that could be considered is the role of 'miners' and how they would be handled under the CSDR in terms of governance and technical requirements given their novel and fundamental role in the settlement process.

149. According to Article 2(f) of SFD, the participants to that system would need to be an institution, a central counterparty, a settlement agent, a clearing house or a system operator. Under the SFD, an institution can be a credit institution, an investment firm, a public authority or publicly guaranteed undertaking, or any undertaking whose head office is outside the Community and whose functions correspond to those of the Community credit institutions or investment firms. This might raise issues, considering that many participants of crypto-asset trading platforms and of DLT networks today are individuals. Some crypto-asset trading platforms might therefore need to re-consider the range of services/activities that they offer to certain types of clients that do not qualify as an institution as defined in the SFD. It should be mentioned that the SFD leaves to the discretion of Member States to broaden the scope of entities that qualify as institutions in some cases, provided that at least three participants to the system are covered by the categories mentioned above, and that such a decision is warranted on grounds of systemic risk.

150. Other important considerations would be that the system and its participants would need to comply with the provisions of Articles 3 to 9 of SFD (transfer and netting legally binding on third parties, rights of holders of collateral security insulated from the effects of the insolvency of the provider, etc.). The system and its participants would also need to comply with the settlement periods and settlement discipline requirements prescribed by Articles 5 to 7 of CSDR (settlement on the intended settlement date and, for transferable securities which are traded on trading venues, no later than on the second business day after the trading takes place, as well as measures to prevent and address settlement fails). We anticipate a number of potential issues in relation to settlement finality and Delivery versus Payment (DvP) in a DLT environment, e.g., how to define and achieve settlement finality with DLT from an operational and legal perspective, considering 'consensus' validation and the risk of 'forks', how to achieve DvP, especially when there is a 'cash' leg that is not processed on DLT. The provision of settlement in central bank money, which is a practice encouraged by CSDR, where practical and available, would also require consideration. The current speed (or variability of speed) with which transactions are completed on DLT under some trading models may pose challenges to fulfil the timeline requirements set by CSDR. An additional issue to be considered is related to access to the system, as well links with other financial market infrastructures and trading venues (traditional or DLT based). Noteworthy, these issues would be heightened for permissionless DLTs as already discussed.

151. Importantly, while providers of CSD type services in a DLT framework should be subject to the same requirements as provided by SFD and CSDR, ESMA believes that consideration would need to be given as to whether and how to tailor the existing rules to address any new issues and risks raised by the technology, also with the objective not to hinder developments that may benefit users.

Lack of a designated securities settlement system

152. If not designated as a securities settlement system under the SFD, the trading platform or underlying DLT may qualify as a settlement internaliser under CSDR. Article 2(1)(11) of CSDR defines a settlement internaliser as any institution which executes transfer orders other than through a securities settlement system.

153. According to Article 9 of CSDR, settlement internalisers shall report to the competent authorities on a quarterly basis the aggregated volume and value of all securities transactions that they settle outside securities settlement systems. The internalised settlement reporting requirements are further specified in the Commission Delegated Regulation (EU) 2017/391, while the reporting templates and procedures are defined in the Commission Implementing Regulation (EU) 2017/393.

154. Noteworthy, SFD would not apply in this case, meaning that investors would not benefit from the safeguards that SFD provides.

Settlement provisions applicable to trading venues

155. Article 6(1) of CSDR provides that trading venues shall establish procedures that enable the confirmation of relevant details of transactions in financial instruments[52] on the date when the transaction has been executed. Article 6(2) provides that notwithstanding the requirements laid down in Article 6(1) authorised investment firms shall, where applicable, take measures to limit the number of settlement fails. Such measures shall at least consist of arrangements between the investment firms and its professional clients to ensure the prompt communication of an allocation of securities to the transaction, confirmation of that allocation and confirmation of the acceptance or rejection of terms in good time before the intended settlement date. Those crypto-assets trading platforms that qualify as RMs, MTFs, OTFs or investment firms will therefore need to fulfil these requirements.

VII.5.2 Book-entry form requirements

156. According to Article 3(1) of CSDR, an issuer established in the Union that issues or has issued transferable securities which are admitted to trading or traded on trading venues shall arrange for such securities to be represented in book-entry form. This requirement shall apply from 1 January 2023 to transferable securities issued after that date and from 1 January 2025 to all transferable securities.

157. According to Article 3(2) of CSDR, where a transaction in transferable securities takes place on a trading venue the relevant securities shall be recorded in book-entry form in a CSD. Where transferable securities are transferred following a financial collateral arrangement as defined in point (a) of Article 2(1) of Directive 2002/47/EC, those securities shall be recorded in book-entry form in a CSD on or before the intended

[52] Financial instruments referred to in Article 5(1) of CSDR, i.e. transferable securities, money-market instruments, units in collective investment undertakings and emission allowances.

settlement date, unless they have already been so recorded. These requirements are already applicable.

158. Recital 11 of the CSDR provides that the Regulation should not impose one particular method for the initial book-entry form recording which should be able to take the form of immobilisation or of immediate dematerialisation. Immobilisation and dematerialisation should not imply any loss of rights for the holders of the securities and should be achieved in a way that ensures that holders of securities can verify their rights.

159. Based on the above, where crypto-assets qualify as transferable securities and are traded on trading venues, their issuer, provided it is established in the Union, shall arrange for such securities to be represented in book-entry form with an authorised CSD as defined under Article 2(1) of CSDR. Other than the reference to the use of 'securities accounts'[53], CSDR does not prescribe any particular method for the initial book-entry form recording, meaning that any technology, including DLT, could virtually be used, provided that the book-entry form is with an authorised CSD. However, there may be national rules that could pose restrictions to the use of DLT for that purpose. The legal nature of a securities account (i.e. statutory record, contractual construct or accounting device) and the legal nature and effects of book entries are still embedded in national law.

160. In order to enhance asset protection, CSDR requires CSDs to segregate the securities accounts maintained for each participant and offer, upon request, further segregation of the accounts of the participants' clients. CSDs and their participants are required to provide for both omnibus client segregation and individual client segregation so clients can choose the level of segregation they believe is appropriate to their needs.

161. The recording of securities in book-entry form is an important step towards increasing the efficiency of settlement and ensuring the integrity of a securities issue, especially in a context of increasing complexity of holding and transfer methods. CSDs play a key role in facilitating the timely settlement of securities transactions, and in ensuring the integrity of the securities issue (including, according to Article 37 of CSDR, through daily reconciliation measures involving the CSD's participants as well as other relevant entities, such as the issuer, registrars, etc.). Crypto-assets trading platforms that qualify as RMs, MTFs, OTFs or investment firms may be subject to the reconciliation measures under CSDR.

VII.6 Safekeeping and record-keeping of ownership of securities and rights attached to securities

162. There is no harmonised definition of safekeeping and record-keeping of ownership of securities at EU-level and this task is performed by a wide range of entities such as custodian banks, registrars, notaries, depositaries or CSDs. The rules also depend on whether the record-keeping applies at the issuer level (notary function) or

[53] Article 2(1) (28) of the CSDR defines a securities account generically as "an account on which securities may be credited or debited".

investor level (custody/safekeeping function). At the issuer level, the rules are dependent on each national corporate law. At the investor level, depending on the type of investor, the rules will vary across several sectorial legislations such as MiFID II or the UCITS V Directive/ AIFM Directive.

163. CSDR requirements may also apply in relation to the initial recording of securities in a book-entry system (notary service), providing and maintaining securities accounts at the top tier level (central maintenance service), or providing, maintaining or operating securities accounts in relation to the settlement service, establishing CSD links, collateral management. The Financial Collateral Directive (FCD) may also apply if the crypto-assets qualify as assets that can be subject to financial collateral arrangements as defined in the SFD. Moreover, the rules will also vary according to the national legislation applicable to securities and the rights attached to securities, which is not harmonised at EU level.

164. When it comes to crypto-assets, a first issue that arises is about the interpretation of what constitutes safekeeping services. ESMA's preliminary view is that having control of private keys on behalf of clients might be regarded as safekeeping services and that rules to ensure the safekeeping and segregation of client assets should apply to the providers of those services. Yet, this requires further consideration, as other criteria may be relevant to qualify these services and the 'holding of private keys on behalf of clients' may take different forms and therefore have different legal meanings. Multi-signature wallets, where several private keys held by different individuals instead of one are needed for a transaction to happen, will also require consideration. Regulators should then consider the contents of these rules and the way in which they might be fulfilled in a DLT environment. This also applies to the requirements provided for investment firms that hold financial instruments belonging to clients under Article 16(8) of MiFID 2.

VII.7 AIFMD

165. the Alternative Investment Fund Managers Directive (AIFMD) [54] lays down requirements for the authorisation, organisation, business conduct and transparency of managers of alternative investment funds (AIFMs) which manage and/or market alternative investment funds (AIFs) in the Union.

166. Several NCAs responding to ESMA's survey on the legal qualification of crypto-assets (see Annex 1) expressed the view that some crypto-assets may qualify as units in collective investment undertakings, most likely AIFs. Further analysis will be required to assess whether those cases may fall within the scope of the AIFMD and therefore need to comply with AIFMD rules.

[54] Directive 2011/61/EU

VII.8 Directive on investor-compensation schemes

167. The Directive on investor-compensation schemes [97/9/EC] provides access to compensation up to a specified amount for investors where the investment firm is no longer financially able to meet its obligations and requires all authorised investment firms to belong to such a scheme. It applies to MiFID firms in relation to MiFID financial instruments.

VII.9 The fifth AMLD on money laundering and terrorist financing

168. In the July 2014 Opinion 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. Legislative amendments to this effect were ultimately agreed in the context of the AMLD5 negotiations such that providers engaged in exchange services between VCs and *fiat* currencies as well as custodian wallet providers are 'obliged entities' within the scope of the AMLD. The AMLD5 is required to be implemented into national law by 10 January 2020.

169. Since the EBA's 2014 Opinion, services such as crypto-to-crypto exchanges (whereby one crypto-asset can be exchanged for another type of crypto-asset) have become more prevalent. ESMA therefore agrees with the recommendation set by the EBA in its report and advice on crypto-assets that the scope of the AMLD should be reviewed in light of these developments and the recommendations of the Financial Action Task Force (FATF) of October 2018 to have within the scope of AML/CFT obligations: (i) providers of exchange services between crypto-assets and *crypto-assets;* and (ii) providers of financial services for ICOs.

VIII. Gaps and issues for consideration by EU policymakers

170. This section outlines the gaps and issues that ESMA has identified in the course of its work, and possible ways to address them through legislation for consideration by the Commission and the co-legislators. The section first discusses those gaps, issues and possible ways to address them when crypto-asset qualify as MiFID financial instruments. It then discusses gaps, issues and possible ways to address them when crypto-assets do not qualify as MiFID financial instruments. Importantly, because DLT is still at an early stage and the business models are evolving, ESMA believes that these gaps, issues and recommendations will need to be re-assessed as the phenomenon develops.

VIII.1 Potential gaps and issues in the existing EU financial services rules when crypto-assets qualify as MiFID financial instruments

171. Where crypto-assets qualify as transferable securities or other types of MiFID financial instruments, a full set of rules is likely to apply to them and to firms providing

investment services/activities in relation to those instruments as discussed in section VII above. The vast majority of NCAs agree with this assessment as highlighted in the ESMA survey. However, because the existing regulatory framework was not designed with these instruments in mind, NCAs face challenges in interpreting the existing requirements and these may therefore not apply consistently across Member States, at the risk of creating regulatory arbitrage. In addition, there are gaps and issues in the current rules, e.g., rules that leave certain risks unaddressed or that may not be adapted to DLT. ESMA believes that these issues need to be considered and, if appropriate, addressed by the Commission and the co-legislators.

172. First, ESMA believes that greater clarity around the types of services/activities that may qualify as custody/safekeeping services/activities under EU financial services rules in a DLT framework is needed. ESMA's preliminary view is that having control of private keys on behalf of clients could be the equivalent to custody/safekeeping services, and the existing requirements should apply to the providers of those services. Meanwhile, there may be a need to consider some 'technical' changes to some requirements and/or to provide clarity on how to interpret them, as they may not be adapted to DLT technology.

173. Second, greater certainty around the concepts of settlement and settlement finality applied to crypto-assets is needed. ESMA believes that there may be a need to distinguish between permissioned and permissionless DLTs in that respect. In particular, ESMA has identified specific governance issues with permissionless DLTs, which makes them less suitable to the processing of financial instruments, at least in their current form. Another related issue is the role of 'miners' and how they would be handled under the existing rules given their novel and fundamental role in the settlement process.

174. Third, ESMA has identified risks that are specific to the underlying technology that might require new/enhanced requirements. In particular, ESMA believes that there should be a means to ensure that the protocol and smart contracts underpinning crypto-assets and crypto-asset activities meet minimum reliability and safety requirements. More generally, the novel cyber security risks, including the risks of hacks, posed by DLT should be considered, to assess whether they are appropriately addressed by the existing set of rules.

175. In ESMA's view the above gaps and issues would require Level 1 measures, which could be complemented by Level 2 technical standards, followed by Level 3 measures adopted by ESMA.

176. Other gaps and issues that require consideration include:

- For those platforms trading crypto-assets, there is a lack of clarity on how to apply the existing rules to so-called decentralised and hybrid models that use smart contracts to match orders and/or conclude transactions, as a platform operator may not exist as such. Extending MiFID 2/MiFIR to at least some of those trading platforms would require either a brand new section in the Level 1 text or an amendment to the current definition of multilateral trading venue and

the various types of trading models available. This would in turn require an extensive review of the related Regulatory Technical Standard and Q&A published to assess how they would be impacted by the revised definition provided in MiFID 2/MiFIR. Alternatively, if a separate definition of crypto-asset trading platform was provided in Level 1, this will also likely require dedicated Level 2 measures requiring significant technical expertise. As this is a still new and evolving area, it can also be expected that ESMA will be required to produce substantial level 3 guidance.

- ESMA believes that some amendments to the pre- and post-trade transparency requirements applicable to venues trading crypto-assets are needed, as the current requirements are tailored to traditional financial instruments. This would require amendments to MiFIR Level 1 legislation and related Level 2 provisions. In the first place, any meaningful pre- or post-trade transparency requirements would have to be based on a shared understanding of the type of crypto assets traded. In addition, as pre- and post- trade transparency requirements are currently based on liquidity and size-of the order/transaction criteria, this would require setting out liquidity thresholds and size thresholds at Level 2 for those new instruments, which would represent a significant challenge should the same approach continue to prevail.

- The impacted market participants will not be able to comply with the data reporting requirements before the respective Regulatory Technical Standards relative to various data reporting and record keeping requirements (e.g. transaction reporting, instrument reference data, transparency and DVC data, orderbook data, etc.) are revisited. As the regulations on reporting were designed to capture traditional instruments and not crypto-assets, the information to be reported as per the existing rules might be not sufficient/appropriate to describe the particularities of crypto assets and transactions in those; thus, hindering the fulfilment of the objectives of the respective regulatory reporting regimes. Certain supervisory convergence tools and measures (guidelines and Q&As) would also need to be revisited to provide the clarity on the issues related to crypto-assets.

- Also, the current reporting regimes heavily rely on common identifiers and classifications (e.g. ISO 6166 ISIN code, ISO 10962 CFI code, ISO 4217 currency code) that have not yet been adapted to the new developments in the crypto-assets domain. The CFI code is a cornerstone of many reporting regimes that allows to prescribe precise rules for data reporting, validation and processing dependant on specific classification of instruments, taking into account distinct characteristics of different asset classes. As of now, this standard does not envisage a specific classification of crypto-assets and does not allow for differentiating them from traditional instruments, nor distinguishing between various crypto-assets and their specific characteristics. Similarly, the ISIN code that uniquely identifies each financial instrument and is mandatory for reporting under, among others, MiFID 2/MiFIR and MAR regimes, currently is not being assigned to crypto-assets. The respective ISO committees consider

developing a new standard for the identification of digital assets, however such work is still ongoing. Until the application of the classification and identification standards for crypto-assets is adapted and the business processes for issuing those codes are established, the market participants will not be able to obtain the codes required by the regulations and thus will not be able to comply with the applicable reporting requirements.

- Finally, the above changes that are required in regulations and data standards imply that the reporting messages will need to be updated and the overall community of participants to the regulatory reporting process (i.e. market participants, market infrastructures and competent authorities) will need to adapt their reporting systems. Moreover, the population of market participants falling under the scope of comprehensive data reporting requirements will grow and they will need to develop capacity to comply with those requirements.

- Further analysis on the interaction between crypto-assets qualifying as financial instruments and other financial instruments would be needed to determine whether there are gaps with respect to MAR and the SSR. In particular, it would be convenient to analyse (i) MAR to ensure the adequacy of the existing provisions to address the potential risks raised by crypto-assets and (ii) the list of financial instruments in Annex I of Commission Delegated Regulation (EU) 918/2012) to ensure that those crypto-assets that might generate a net short position on a share or on a sovereign debt are explicitly included in that list.

177. Finally, the results of the Survey made clear that the Member State NCAs in the course of transposing MiFID into their national laws, have in turn defined the term financial instrument differently. While some employ a restrictive list of examples to define transferable securities, others use broader interpretations. This creates challenges in both in the regulation and supervision of crypto-assets.

VIII.2 Potential gaps and issues in the existing EU financial services rules when crypto-assets do not qualify as MiFID financial instruments

178. The size of the crypto-asset market remains relatively modest and ESMA does not believe that it currently raises financial stability issues, although the development of the sector requires monitoring. However, ESMA is concerned about the risks that crypto-assets represent to investor protection. ESMA identifies the most significant risks as potentially stemming from fraud, cyber-attacks, and money laundering and market manipulation.

179. There are a wide range of crypto-assets being issued and only a fraction of them are likely to qualify as MiFID financial instruments. Where crypto-assets do not qualify as MiFID financial instruments and unless they qualify as electronic money[55], they are

[55] See footnote 3

likely to fall outside of the existing EU financial services rules, in which case investors will not benefit from the safeguards that these rules provide. Meanwhile, investors may not easily distinguish between those crypto-assets that are within the scope of EU financial services rules and those that are not, especially when they are available for trading on the same venues.

180. ESMA is aware that some Members States have or are considering bespoke regimes for those crypto-assets that do not qualify as MiFID financial instruments. While ESMA understands the intention to provide for both a protective and supportive approach to these instruments, ESMA is concerned that this does not provide for a homogeneous framework across the EU.

181. Against this background, ESMA foresees the following two options:

Option A: Implement a bespoke regime for specific types of crypto-assets

182. EU policymakers could consider the opportunity to set up a bespoke regime for those crypto-assets that do not qualify as financial instruments. Such a bespoke regime, which would require Level 1 measures, would allow tailoring the rules to the specific risks and issues posed by those crypto-assets that do not qualify as financial instruments or electronic money. It may also provide for different requirements depending on the features of these crypto-assets, as some may be further away from traditional financial instruments than others and therefore not raise the same risks and issues, e.g., 'pure' utility-type crypto-assets, which appear to have little relation to financial markets and can only be redeemed for certain goods or services (e.g. non-tradable vouchers) and certain payment-type crypto-assets.

183. As a priority, in line with EBA's recommendation and ESMA's survey, which highlighted a broad consensus among NCAs that AML rules should apply to all activities involving crypto-assets, ESMA advises EU policymakers to consider reviewing the scope of AML requirements taking account of market developments including with regards to providers of crypto-to-crypto exchange services and providers of financial services for ICOs.

184. In addition, ESMA believes that as a further priority EU policymakers should consider the need to have appropriate risk disclosure requirements in place, including in relation to the issuer, the project, the rights attached to the crypto-asset, the underlying technology used and potential conflict of interest, to ensure that consumers are aware of the risks prior to committing funds to crypto-assets. To date, the quality, transparency and disclosure of risks in so-called ICO 'white papers' varies greatly and often emphasises likelihood of financial returns to encourage speculative 'investment' behaviour by consumers, even where a crypto-asset lacks the legal characteristics to be a financial instrument.

185. Wider regulation of crypto-assets and related activities may have trade-offs, such as risking legitimising crypto-assets and encouraging wider adoption. It will also require further supervisory resources. Any novel framework should also protect the integrity of existing capital markets. Therefore, at this stage, ESMA advises to focus the

regime for crypto-assets that are not financial instruments on warning buyers about the risks of those crypto-assets, instead of a more elaborate regime that could legitimise crypto-assets and bring them into a similar regulatory remit as the one for crypto-assets that are financial instruments.

186. In undertaking this Option, the European Institutions are advised that there exists a wide range of non-financial instrument crypto-assets. In turn, the proposed regime must be supple enough to capture the wide variety of characteristics and risk factors that these non-financial instrument crypto-assets introduce.

187. Any consideration of further regulation may also benefit from an assessment of developments in other major jurisdictions and their regulatory responses, and seeking to develop common responses. To this end, Appendix 5 provides a brief overview of some of the key response of other regulators to date on the emergence of crypto-assets.

Option B: Do Nothing

188. Under this scenario, financial regulators may consider that certain crypto-assets fall outside of their remit, and in turn should take no further action.

189. However, this option fails to address the known investor protection and market integrity concerns. ESMA therefore believes Option A is the most appropriate course of action.

Appendix 1 – Glossary

Information: This glossary sets out a (non-exhaustive) list of terms used in the Advice. It is based on the usage in other ESMA documents, the usage in FSB reports, as well as in the work of the CPMI, Markets Committee, BCBS, and IOSCO.

Blockchain: a form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerised process by which transactions are validated.

Centralised crypto-asset trading platform: a type of crypto-asset trading platform that holds crypto-assets on behalf of its clients. The trade settlement usually takes place in the books of the platforms, i.e. off-chain.

Crypto-asset: a type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT) or similar technology as part of their perceived or inherent value. Unless otherwise stated, ESMA uses the term to refer to both so-called 'virtual currencies' and 'digital tokens'. Crypto-asset additionally means an asset that is not issued by a central bank.

Crypto-asset trading platform: any trading platform where crypto-assets can be bought and sold, regardless of their legal status. Crypto-assets may be traded or exchanged for fiat currencies or other crypto-assets.

Cryptography: the conversion of data into private code using encryption algorithms, typically for transmission over a public network.

Decentralised crypto-asset trading platform: a type of crypto-asset trading platform that does not hold crypto-assets on behalf of its clients but rather provides an infrastructure connecting them. The trade settlement usually takes place on the respective DLT network, i.e. on-chain.

Digital token: any digital representation of an interest, which may be of value, a right to receive a benefit or perform specified functions or may not have a specified purpose or use.

Distributed consensus mechanism: the process of network participants within a DLT environment of agreeing on one state or result of the distributed ledger.

Distributed ledger technology (DLT): a means of saving information through a distributed ledger, i.e., a repeated digital copy of data available at multiple locations. DLT is built upon public-key cryptography, a cryptographic system that uses pairs of keys: public keys, which are publicly known and essential for identification, and private keys, which are kept secret and are used for authentication and encryption.

FinTech: technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services.

Fork: a change to the DLT protocol.

Hard fork: a change to a DLT protocol that requires all nodes or users to upgrade to the latest version of the protocol software, or creates two versions of the protocol going forward.

Initial coin offering (ICO): an operation through which companies, entrepreneurs, developers or other promoters raise capital for their projects in exchange for crypto-assets (often referred to as 'digital tokens' or 'coins'), that they create.

Investment-type crypto-asset: A type of crypto-asset that resembles a financial instrument.

Miners: A network of computers establishing consensus to verify and confirm transactions within a DLT environment. Miners effectively provide the necessary computational power to validate transactions and include them in the next block of transactions in the chain. 'Miners' is an expression often referred to under a 'Proof-of-Work' consensus mechanism.

Payment-type crypto-asset: a type of crypto-asset that is meant to be used as a means of payment or exchange for goods or services that are external to the DLT ecosystem on which they are built.

Permission-based DLT: a DLT network in which only those parties that meet certain requirements are entitled to participate to the validation and consensus process.

Permissionless DLT: a DLT network in which virtually anyone can become a participant in the validation and consensus process.

Proof-of-stake consensus mechanism (PoS): PoS is a form of consensus mechanism within a DLT environment that requests participants to demonstrate ownership of a pre-defined crypto-asset. With PoS, a person can mine or validate block transactions according to how many of the respective crypto-assets he or she holds.

Proof-of-Work consensus mechanism (PoW): PoW is a consensus mechanism within a DLT environment that involves all participants in the consensus process in an extensive 'guessing and checking'-puzzle. Participants in this process compete against each other to be the first to complete transactions in order to get rewarded.

Utility-type crypto-asset: a type of crypto-asset that provides some 'utility' function other than as a means of payment or exchange for external goods or services.

Wallet provider: a firm that offers storage services to investors in crypto-assets. These may be connected online ('hot' storage) or kept offline ('cold' storage).

Appendix 2 – Overview of crypto-asset trading platforms business models

Centralized vs Decentralized platforms

190. Centralized platforms, which seem to be the dominant model today, require users to deposit their assets with the platform prior to trading, which in the case of crypto-assets effectively means to hand over the control of their private keys to the platform prior to trading. Another distinguishing feature of centralized platforms is that only when users deposit/withdraw their crypto-assets at the platform is the transaction usually recorded on DLT (on-chain). The rest, e.g., the matching of orders, the execution of orders and the corresponding transfer of ownership between users, is typically recorded in the books of the platform only (off-chain).

191. This set-up has two major consequences. First, there is a heightened risk of a hack, as these platforms represent a single point of failure where clients' private keys are centrally stored. Indeed, several of those platforms have been hacked with total losses to date exceeding USD 1bn according to Bloomberg.[56] Second, the fact that only the deposit/withdrawal is recorded on-chain means that the settlement of trades is not dependent on DLT, which may have some benefits (no congestion risk, no scalability issue) but downsides as well (counterparty risk vis-à-vis the platform).

192. Decentralized platforms, also known as DEXs, were born from the desire to address the vulnerabilities of centralized platforms by building marketplaces directly on DLT. With DEXs, there is no middleman or central authority. Instead, smart contracts govern the transactions.[57] Yet, DEXs face a number of challenges. They tend to be slower than centralised platforms, as every transaction needs to be processed and validated on DLT, which also bears a cost. They can also introduce new kinds of security vulnerabilities and are technically complex to develop. Fully-fledged DEXs are by design limited to crypto-to-crypto (and not crypto-to-fiat) transactions. ESMA's current understanding is that DEXs are still at an early stage of development.

193. Semi-decentralized exchanges are emerging as hybrid models. In most cases, servers (centralized) still host order books but do not hold private keys.

Order book versus no order book

194. Some platforms use an order book while others do not. As an example, some DEXs use a smart contract or a liquidity pool that simply fills submitted orders algorithmically. Also, the order books may be on-chain or off-chain.

[56] https://www.bloomberg.com/news/articles/2018-01-28/massive-cryptocurrency-heist-puts-spotlight-on-exchange-security, also https://blog.localethereum.com/centralised-exchanges-are-terrible-at-holding-your-money/

[57] See https://medium.com/herdius/decentralized-vs-centralized-exchanges-bdcda191f767

Platforms connecting buyers and sellers

195. Some platforms display trading interests but do not execute orders. They allow buyers and sellers to find each other and then negotiate and agree upon transaction details by communicating directly with each other. Because this framework may leave users vulnerable to fraud, some platforms have introduced security features such as obligatory deposits.[58] Other use atomic swaps which can be on-chain or off-chain.[59] Those are mechanisms to ensure trust by releasing funds and assets when every party to the transaction has fulfilled its obligations. After a period of time the transaction lapses and the funds are returned to the rightful owner.

Broker/dealer type platforms

196. These are websites to buy cryptocurrencies at a price set by the dealer. The dealer buys and sells cryptocurrency by maintaining their own inventory book and setting a bid/offer spread. Transaction times may take up to several minutes so these platforms are not suitable for active trading. In some cases the fees and mark-ups are not revealed.

[58] Before a trade begins, both counterparties have to deposit a certain amount of crypto assets. If the trade completes and no issues arise, those deposits return back to the users. If a dispute arises, an arbitrator appointed by the community hears both sides and resolves it. The deposits are then used to compensate the victim of the fraud and the arbitrator's, see serviceshttps://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained

[59] On-chain atomic swaps take place on either currency's blockchain. Currently, for these swaps to work, both currencies must use the same hashing algorithm, and they also must support HTLC. A Hashed TimeLock Contract or HTLC is a type of conditional payment that uses hashlocks and timelocks to require that the receiver of a payment either acknowledges receiving it prior to a deadline by generating cryptographic proof of payment or forfeit the ability to claim the payment, returning it to the payer, see https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts. Off-chain atomic swaps allow for off-blockchain exchange of a number of selected currencies. This takes place on a secondary layer of nodes.

Appendix 3: Capital requirements for investment firms

Initial capital endowment

The initial capital requirements are set out in Directive 2013/36/EU and Regulation (EU) No 575/2013 (also known as "CRD IV/CRR"). They vary depending on the type of MiFID services/activities, as outlined in Table 1.

Table 1: Categorisation of MiFID investment firms within the CRD framework

	Categories	Initial capital	Own funds requirements
1	Local firms (CRR 4(1)(4))	€50 000 (CRD 30)	Not applicable
2	Firms falling under CRR 4(1)(2)(c) that only provide reception/transmission and/or investment advice	€50 000 (CRD 31(1))	Not applicable
3	Firms falling under CRR 4(1)(2)(c) that only provide reception/transmission and/or investment advice and are registered under the Insurance Mediation Directive (IMD)	€25 000 (CRD 31(2))	Not applicable
4	Firms falling under CRR 4(1)(2)(c) that perform, at least, execution of orders and/or portfolio management	€50 000 (CRD 31(1))	CRR 95(2)
5	Investment firms not authorised to perform deals on own account and/or underwriting/placing with firm commitment that do not hold client funds/securities	€50 000 (CRD (29(3))	CRR 95(1)
6	Investment firms not authorised to perform deals on own account and/or underwriting/placing with firm commitment but hold client funds/securities	€125 000 (CRD 29(1))	CRR 95(1)
7	Investment firms that operate an MTF	€730 000 (CRD 28(2))	CRR 95(1)
8	Investment firms that only perform deals on own account to execute client orders	€730 000 (CRD 28(2))	CRR 96(1)(a)
9	Investment firms that do not hold client funds/securities, only perform deals on own account, and have no external clients	€730 000 (CRD 28(2))	CRR 96(1)(b)
10	Commodity derivatives investment firms that are not exempt under the MiFID	€50 000 to 730 000 (CRD 28 or 29)	CRR 493 & 498
11	Investment firms that do not fall under the other categories	€730 000 (CRD 28(2))	CRR 92

Source : EBA report on investment firms, EBA/Op/2015/20

Appendix 4: Details of organizational requirements under Article 16 of MiFID 2

An investment firm should:

a) maintain and operate an effective organisational and administrative arrangements to taking all reasonable steps designed to prevent conflicts of interest affecting the interests of its clients;

b) Maintain, operate and review a process for the approval of financial instruments before marketed or distributed to clients, including target market, relevant risks and distribution strategy;

c) review regularly the financial instruments offered;

d) make available appropriate information on the financial instrument and the product approval process, including target market;

e) have in place adequate arrangements to obtain the above information if offers financial instruments that they do not manufacture;

f) take reasonable steps to ensure continuity and regularity in the performance of investment services and activities (appropriate and proportionate system, resources and procedures);

g) ensure it takes reasonable steps to avoid undue operational risk in the case of outsourcing of critical functions (internal control and ability to monitor the firms compliance with all obligations needs to remain at the firm);

h) have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment and effective control and safeguard arrangements for information processing systems;

i) have sound security mechanisms to guarantee the security and authentication of the means of transfer of information, minimise risk of data corruption and unauthorized access and to prevent information leakage maintaining the confidentiality of the data at all times;

j) arrange for records to be kept of all services, activities and transactions undertaken which are sufficient to enable the competent authority to fulfil its supervisory tasks to ascertain the investment firm has complied with all relevant obligations;

k) records shall include the recording of telephone conversations or electronic communications relate to transactions concluded when dealing on own account and the provision of client order services that relate to the receptions transmission and execution of client orders.

Appendix 5: Overview of national regimes for crypto-assets

Three countries in Europe have or are considering steps to implement a bespoke national regime for those crypto-assets that are not covered by the existing EU framework.

France

The French government is in the process to adopt a bespoke opt-in regime for ICOs, following the consultation from the AMF.[60] The article 26 of the PACTE law makes reference to ICOs and a voluntary regime for crypto-assets. According to the proposal the French AMF will approve 'utility' ICOs that meet certain minimum requirements in relation to disclosure information, funds security and AML. This 'white list' approach will be complemented with a 'black list' approach, whereby the AMF will be empowered with enforcement actions against fraudulent ICOs. The AMF sees this opt-in regime as a transition phase, which might become mandatory in the future. In addition, the AMF is discussing a regime for secondary trading platforms with the Ministry and ACPR. The regime will need to address three key areas, namely (i) trading through platforms that look like MTF; (ii) brokerage services; and (iii) safekeeping. The AMF is also considering some possible additional customer protection provisions, e.g., banning active marketing of crypto-assets to retail. The first lecture of the law took place in the National Assembly last October and in November it will proceed in the Senate, it is expected that the law would approved in 2019.[61]

Liechtenstein

Liechtenstein has published the Unofficial Translation of the Draft-Law on Transaction Systems Based on Trustworthy Technologies (Blockchain Act).[62] Currently the act is in consultation period until mid-November. The following steps to adopt the draft VTG would be for it to be brought forward with a reasoned 'report and application' (Bericht und Antrag), opening debate with general discussion and a first reading in the parliament, the statement of the government and a second reading with following final poll. The purpose of the act is to 'protect users on IT Systems and to ensure their trust in digital rights'. The aim is to promote a positive development of the token economy in Liechtenstein, ensuring legal certainty. The draft law contains provisions on trusted technologies, definitions as the one of tokens, rights of disposal, requirements for VT service providers, basic information on the issuance of tokens, obligation to register, supervision and penal provisions.[63]

---

[60] AMF, 2018, "Summary of replies to the public consultation on Initial Coin Offerings (ICOs) and update on the UNICORN Programme". Available at http://www.amf-france.org/en_US/Publications/Consultations-publiques/Archives?docId=workspace%3A%2F%2FSpacesStore%2Fa9e0ae85-f015-4beb-92d2-ece78819d4da&langSwitch=true

[61] https://www.economie.gouv.fr/plan-entreprises-pacte

[62] http://www.regierung.li/media/attachments/VNB-Blockchain-Gesetz-en-full-clean.pdf?t=636777232664164584

[63] https://www.pwc.ch/en/insights/regulation/liechtenstein-publishes-draft-of-the-new-blockchain-act.html

Malta

The Parliament in Malta approved three acts in July, effectively setting-up a bespoke framework for ICOs and DLT-related activities. The three acts were the Malta Digital Innovation Authority (MDIA) Act,[64] the Innovative Technology Arrangements and Services (ITAS) Act,[65] and the Virtual Financial Asset (VFA) Act that regulates ICOs, VCs and service providers involved in ICOs and other VC activities that fall outside of the existing regulatory framework. [66] Christopher P. Buttigieg & Christos Efthymiopoulos, both from the Malta Financial Services Authority produced an explanatory article about the VFA Act that provides an insight on the regulation.[67]The article focuses on the key features of the Malt's Virtual Financial Assets Act, explaining the initial VFA offering, the status of services providers, the role of VFA agents and the measures for AML and combating funding of terrorism. The authors highlighted that investor protection, market integrity and financial soundness would need further cooperation between countries to be ensured. Noticeably, almost two-thirds of the agent qualification have failed which has been understood as an indicator that certain industry players are not prepared to register as VFA agents as was previously reported by a MSFA consultation document.[68] [69]

[64] Malta, 2018, MDIA Act. Available at http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1
[65] Malta, 2018, ITAS Act. Available at http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1
[66] Malta, 2018, VFA Act. Available at http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29201&l=1
[67] Christopher P. Buttigieg & Christos Efthymiopoulos (2018): The regulation of crypto assets in Malta: The Virtual Financial Assets Act and beyond, Law and Financial Markets Review.
[68] https://cointelegraph.com/news/malta-two-thirds-fail-crypto-agent-exam-despite-authorities-attempts-to-ease-process
[69] https://www.mfsa.com.mt/.../20180904_VFA_VFAAgentsRaisingtheBar.pdf