Public consultation an EU framework for markets in crypto-assets

Response of FG Lawyers

For more information, please contact:

Anne Hakvoort

T: +31 (0)20 7603137

@: hakvoort@fglawyersamsterdam.com

www.fglawyeramsterdam.com

I. Classification of crypto-assets

There is not a single widely agreed definition of 'crypto-asset'13. In this public consultation, a crypto-asset is considered as "a digital asset that may depend on cryptography and exists on a distributed ledger". This notion is therefore narrower than the notion of 'digital asset'14 that could cover the digital representation of other assets (such as scriptural money).

While there is a wide variety of crypto-assets in the market, there is no commonly accepted way of classifying them at EU level. This absence of a common view on the exact circumstances under which crypto-assets may fall under an existing regulation (and notably those that qualify as 'financial instruments' under MiFID II or as 'e-money' under EMD2 as transposed and applied by the Member States) can make it difficult for market participants to understand the obligations they are subject to. Therefore, a categorisation of crypto-assets is a key element to determine whether crypto-assets fall within the current perimeter of EU financial services legislation.

Beyond the distinction 'regulated' (i.e. 'security token', 'e-money token') and unregulated crypto-assets, there may be a need for differentiating the various types of crypto-assets that currently fall outside the scope of EU legislation, as they may pose different risks. In several Member States, public authorities have published guidance on how crypto-assets should be classified. Those classifications are usually based on the crypto-asset's economic function and usually makes a distinction between 'payment tokens' that may serve as a means of exchange or payments, 'investment tokens' that may have profit-rights attached to it and 'utility tokens' that enable access to a specific product or service. At the same time, it should be kept in mind that some 'hybrid' crypto-assets can have features that enable their use for more than one purpose and some of them have characteristics that change during the course of their lifecycle.

[13] This section concerns both crypto-assets that fall under existing EU legislation (those that qualify as 'financial instruments' under MiFID II and those qualifying as 'e-money' under EMD2) and those falling outside.

[14] Strictly speaking, a digital asset is any text or media that is formatted into a binary source and includes the right to use it.

Question 5. Do you agree that the scope of this initiative should be limited to crypto-assets (and not be extended to digital assets in general)?

Yes. The FATF refers in its recommendations to virtual assets (which is, in our view, the same as digital assets). EBA and ESMA on the other hand seem to focus (or limit?) on the term crypto asset. If the definition of the FATF is followed in respect of digital assets ("a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. […]", we would be in favour of extending the scope of this exercise to virtual assets. However, if the explanation of a digital asset as included in footnote 14 above is followed, such digital asset not necessarily relates to financial markets; in that definition a digital asset it is not necessarily a financial product which requires a financial regulatory framework. The first important step is to introduce European or preferably global definitions of these terms (digital assets, virtual assets (if different), crypto assets). In our view only a financial regulatory framework should apply to such digital/virtual/crypto assets that actually function within the financial markets. Within that framework, the (now known) different appearances of such digital/virtual/crypto assets should be determined and in respect of each such appearance it should be clarified whether or not such appearance falls under a financial regulatory framework (existing or to be developed). We think it will be challenging enough to differentiate between the different types and appearances of crypto assets and to formulate a proper regulatory framework around these (or to provide guidance/clarification as regards the applicability of the current regulatory framework to such different types of crypto assets). Extending this exercise to digital assets as meant in footnote 14 above, will make it an almost impossible task. Since these developments go quickly, it is of the essence that the focus will be on a rather speedy legislative or similar procedure instead of losing time discussing issues which may not be of clear relevance for a financial regulatory framework.

Question 6. In your view, would it be useful to create a classification of crypto-assets at EU level? If yes, please indicate the best way to achieve this classification (non- legislative guidance, regulatory classification, a combination of both, ...).

Yes. In order to speed up, presumably the issuance of non-legislative guidance should be issued as soon as possible. We would not be surprised if many types of crypto-assets could already be subjected to an existing regulatory framework, such as MiFID II, the Prospectus Regulation, PSD2 and EMD2, AIFMD etc. by no or limited amendment to the definitions used in such European legislation.

We would favour a similar approach as suggested in the proposed Crowdfunding Regulation in respect of a 'MiFID light' regime to which issuers of crypto-assets or other 'crypto assets services providers' (such as custodial wallet providers, exchanges and other intermediaries/brokers in respect of crypto-assets) would be subjected. With reference to our prior responses to FinTech related consultations, we opt for a 'base authorisation/license requirement' for any party - acting in the course of its business - offering any type of financial services in respect of financial products which could be topped up on the basis of volume indicators, such as turnover, assets under management, number of employees, number of clients, etc. This would ensure visibility of any such financial undertaking with the NCAs, whilst also ensuring a proportionate regulatory framework applicable to such financial undertaking. Its license would 'grow' (e.g. on an annual basis if underlying volume indicators have changed) with the financial undertaking. I realize that this is a 180 degree different approach than currently used in the EU and therefore most probably not a path that the EU would be willing to consider, but perhaps it could be introduced for FinTech start ups, including 'crypto assets services providers' if their services do not evidently fall under the scope of already existing EU legislation (though preferably with a more proportionate way of access to the markets without giving in in respect of consumer protection).

To the extent one or more categories of crypto-assets could not be easily brought under the scope of the existing regulatory framework, next to such guidance as mentioned in the first paragraph, due to the cross-border ability of crypto assets by nature, it is of utmost importance as well that there will be an harmonized and convergent regulatory framework in all Member States, limiting the possibility for national legislation to deviate from such EU framework. In that sense, we would highly encourage a regulation over a directive.

Question 7. What would be the features of such a classification? When providing your answer, please indicate the classification of crypto-assets and the definitions of each type of crypto-assets in use in your jurisdiction (if applicable).

As per today's date, no Dutch law includes a definition of crypto assets. In the draft bill amending the Dutch AML Act in relation to the implementation of AMLD 5, a definition for virtual currencies is included. This definition is exactly in line with the definition of virtual currencies as included in AMLD5. The Dutch financial regulators, the Dutch Central Bank and the Netherlands Authority for the Financial Markets, also use this definition in their joint report included recommendations on a regulatory framework applicable to cryptos (available here: https://www.afm.nl/en/nieuws/2019/jan/adviesrapport-crypto). Within this definition, the Dutch NCAs make the distinction between 'transaction cryptos', 'utility cryptos' and 'investment cryptos'. The Dutch NCAs also describe numerous 'crypto related activities' in their report, which may be useful to take into account when thinking of a regulatory framework applicable to crypto assets.

With reference to our answer to question 5 above, we suggest clarifying if 'virtual currencies' are just one classification of crypto assets. Another clarification that we would appreciate is whether 'crypto assets' are only cryptographically encrypted virtual/digital assets, or that it is not intended to limited the applicability of a potential regulatory framework on such virtual/digital assets being encrypted or not.

Question 8. Do you agree that any EU classification of crypto-assets should make a distinction between 'payment tokens', 'investment tokens', 'utility tokens' and 'hybrid tokens'? If you do agree that any EU classification of crypto-assets should make a distinction between 'payment tokens', 'investment tokens', 'utility tokens' and 'hybrid tokens', please indicate if any further sub- classification would be necessary.

Yes and no. When crypto assets only relate to tokens, you miss out on the 'native coins' such as bitcoin. Or it should be clarified that the term token includes such coins as well. However, at the same time it will be extremely difficult to differentiate between these classifications in respect of the regulatory framework applicable to them, as they may change over time. Bitcoin is a perfect example of such change. Originally intended to be a payment crypto, it developed into an investment crypto and therefore could now be qualified as a hybrid crypto. What is important in that respect; what the issuer intended it to be or how the markets / holders use it and which meaning they give to it? Another challenge is that DLT enables crypto assets to be easily tradable. That results, in our view, that those crypto assets that offer similar rights as regular equity and debt securities, to qualify as securities (and therefore financial instruments) within the meaning of MiFID II and the Prospectus Regulation. Will exchanges and other crypto asset services providers offering brokerage and other 'MiFID' services automatically fall under the scope of MiFID II? Will exchanges be qualified as trading venues, requiring a MiFID license for operating such a trading facility? What if, upon issuance, a token is clearly not a security, but develops over time to be an investment token. Would that impact the regulatory framework applicable to such token and the services providers in respect of those tokens?

To this end, we give into consideration to choose for a regulatory framework applicable to crypto assets in its generality, applicable to issuers as well as (professional) crypto services providers offering their services to clients and - in a proportionate manner - cherry picking from the existing regulatory framework (comparable to the proposed Crowdfunding Regulation) and enable incumbents to extent their existing license under MiFIDII, CRDIV, etc to offer their services in relation to crypto assets as well. It could be considered to introduce a new category of financial instrument in MiFID II, being crypto assets though clarifying that the mere offering of investment services or investment activities in respect of crypto assets only does not require a full MiFID II license but, for example a 'MiFID light' license comparable to the license obligation proposed for crowdfunding services providers in the Crowdfunding Regulation.

Back end systems making use of DLT and crypto assets to facilitate a speedy and more robust back end administrative system should be excluded in our view as long as such crypto assets are not meant to be used in such manner by front end users.

The Deposit Guarantee Scheme Directive (DGSD) aims to harmonise depositor protection within the European Union and includes a definition of what constitutes a bank 'deposit'. Beyond the qualification of some crypto-assets as 'e-money tokens' and 'security tokens', the Commission seeks feedback from stakeholders on whether other crypto-assets could be considered as a bank 'deposit' under EU law.

Question 9. Would you see any crypto-asset which is marketed and/or could be considered as 'deposit' within the meaning of Article 2(3) DGSD?

Currently not because there are no crypto assets yet which have the same value as scriptural money etc. which could be deposited with a bank. However, I can imagine this changes over time. In particular if the ECB or national Central Banks would be issuing stable coins or alike instruments, it would in our perception be yet another type of fund within the meaning of PSD2. In that case, in our view any such crypto-assets stored with a credit institution should treat such crypto assets in line with the DGSD resulting in such crypto- assets could qualify as deposits within the meaning of Article 2(3) DGSD.

II. Crypto-assets that are not currently covered by EU legislation

*This section aims to seek views from stakeholders on the opportunities and challenges raised by crypto-assets that currently fall outside the scope of EU financial services legislation[15] (**A.**) and on the risks presented by some service providers related to crypto-assets and the best way to mitigate them (**B.**). This section also raises horizontal questions concerning market integrity, Anti-Money laundering (AML) and Combatting the Financing of Terrorism (CFT), consumer /investor protection and the supervision and oversight of the crypto-assets sector (**C.**).*

[15] Those crypto-assets are currently unregulated at EU level, except those which qualify as 'virtual currencies' under the AML /CFT framework (see section I.C. of this document).

A. General questions: Opportunities and challenges raised by crypto-assets

Crypto-assets can bring about significant economic benefits in terms of efficiency improvements and enhanced system resilience alike. Some of those crypto-assets are 'payment tokens' and include the so-called "stablecoins" (see below) which hold the potential to bridge certain gaps in the traditional payment systems and can allow for more efficient and cheaper transactions, as a result of fewer intermediaries being involved, especially for cross-border payments. ICOs could be used as an alternative funding tool for new and innovative business models, products and services, while the use of DLT could make the capital raising process more streamlined, faster and cheaper. DLT can also enable users to 'tokenise" tangible assets (cars, real estate) and intangible assets (e.g. data, software, intellectual property rights, ...), thus improving the liquidity and tradability of such assets. Crypto-assets also have the potential to widen access to new and different investment opportunities for EU investors. The Commission is seeking feedback on the benefits that crypto-assets could deliver.

Question 10. In your opinion, what is the importance of each of the potential benefits related to crypto-assets listed below?

	1 (not important at all)	2	3	4	5 (very important)	Don't know / no opinion / not relevant
Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs	○	○	◉	○	○	○
Issuance of utility tokens as an alternative funding source for start-ups	○	○	○	◉	○	○
Cheap, fast and swift payment instrument	○	○	○	○	◉	○
Enhanced financial inclusion	○	○	○	◉	○	○
Crypto-assets as a new investment opportunity for investors	○	○	○	◉	○	○
Improved transparency and traceability of transactions	○	○	○	○	◉	○
Enhanced innovation and competition	○	○	○	○	◉	○
Improved liquidity and tradability of tokenised 'assets'	○	○	○	◉	○	○
Enhanced operational resilience (including cyber resilience)	○	○	○	○	◉	○
Security and management of personal data	○	○	○	◉	○	○
Possibility of using tokenisation to coordinate social innovation or decentralised governance	○	○	◉	○	○	○

Reasoning: Crypto assets are just one example of the technological developments that we will face in the era. Instead of closing our eyes for it, we should embrace it and make sure that the manner in which such developments are introduced in the financial markets are done in a proper, prudent and adequate manner. Cyber resilience is of the utmost importance.

Another potential benefit related to crypto assets not mentioned above is accessibility of investment opportunities to retail investors (though we do emphasize that for that reason clarity in respect of the legal framework applicable is very important).

Despite the significant benefits of crypto assets, there are also important risks associated with them. For instance, ESMA underlined the risks that the unregulated crypto-assets pose to investor protection and market integrity. It identified the most significant risks as fraud, cyber-attacks, money-laundering and market manipulation[16]. Certain features of crypto-assets (for instance their accessibility online or their pseudo-anonymous nature) can also be attractive for tax evaders. More generally, the application of DLT might also pose challenges with respect to protection of personal data and competition[17]. Some operational risks, including cyber risks, can also arise from the underlying technology applied in crypto-asset transactions. In its advice, EBA also drew attention to the energy consumption entailed in some crypto-asset activities. Finally, while the crypto-asset market is still small and currently pose no material risks to financial stability[18], this might change in the future.

[16] ESMA, "Advice on initial coin offerings and Crypto-Assets", January 2019.

[17] For example when established market participants operate on private permission-based DLT, this could create entry barriers.

[18] FSB Chair's letter to G20 Finance Ministers and Central Bank Governors, Financial Stability Board, 2018.

Question 11. In your opinion, what are the most important risks related to crypto-assets?

	1 (not important at all)	2	3	4	5 (very important)	no opinion / not relevant
Fraudulent activities	○	○	○	◉	○	○
Market integrity (e.g. price, volume manipulation, ...)	○	○	○	◉	○	○
Investor/consumer protection	○	○	○	○	◉	○
Anti-money laundering and CFT issues	○	○	○	◉	○	○
Data protection issues	○	○	◉	○	○	○
Competition issues	○	◉	○	○	○	○
Cyber security and operational risks	○	○	○	○	◉	○
Taxation issues	○	○	◉	○	○	○
Energy consumption entailed in crypto-asset activities	○	○	○	◉	○	○
Financial stability	○	○	○	○	◉	○
Monetary sovereignty/monetary policy transmission	○	○	○	○	◉	○

Reasoning: We have great trust in DLT and in the potential of crypto assets subject to those crypto assets being offered and services in a prudent manner. If there is a clear (global) regulatory framework applicable to crypto assets, in our view the risks around fraudulent activities and any other criminal use or misuse of these assets are presumably lower than for example with cash money thanks for the, in principle, immutable transparent register of transactions in such crypto assets on a blockchain. We would be in favour, also in order to limit the potential reporting obligations of certain 'crypto asset providers', of granting certain regulatory or governmental authorities (on a national, European or even global scale) with monitoring rights in respect of all transactions that take place on blockchains, irrespective of whether these are public / permissionless blockchains or non-public / permissioned blockchains. AI and similar technologies should be used to fully automatically review all such transactions to pick out irregular or peculiar transactions. Lastly, the gatekeepers role within the meaning of AMLD 5 should be applicable to any 'crypto asset provider' in order to ensure that any person using any type of crypto asset will at least by identified in order to limit AML and CFT risks as much as possible. However, transaction monitoring under AMLD 5 should be done in the above mentioned manner rather than by each gatekeeper involved in crypto assets individually fall. In order to facilitate such KYC/CDD processes, any person should obtain a digital ID, ideally issued by a national authority (comparable to the issuances of regular passports), which any person can use when making use of financial services. Changes in the UBO registers should automatically update one's digital ID. In addition to the UBO register, a PEP register could be introduced having the same functioning as the UBO register.

11.1 Is there any other important risks related to crypto-assets not mentioned above that you would foresee?

Incapability of stakeholders involved, including advisors, NCAs, service providers and users/investors, in really understanding the crypto assets, the algorithm(s) underlying the crypto assets, and the manner in which such underlying technology is used and develops in respect of crypto assets. In terms of professional competence requirements applicable to certain 'crypto service providers' (such as advisors or asset managers), these should include technological competences as well such as a base course in programming etc.

Human responsibility for the (development of the) underlying technology used; at all times the crypto asset and its working should be explainable in easily comprehensible 'human language': AI, machine learning, deep learning and other self learning algo's and algo's interacting on each other should only be a facilitator rather than a creator of (the functionalities of) crypto assets.

"*Stablecoins" are a relatively new form of payment tokens whose price is meant to remain stable through time. Those "stablecoins" are typically asset-backed by real assets or funds (such as short-term government bonds, fiat currency, commodities, real estate, securities, ...) or by other crypto-assets. They can also take the form of algorithmic "stablecoins" (with algorithm being used as a way to stabilise volatility in the value of the coin). While some of these "stablecoins" can qualify as 'financial instruments' under MiFID II or as e-money under EMD2, others may fall outside the scope of EU regulation. A recent G7 report on 'investigating the impact of global stablecoins' analysed "stablecoins" backed by a reserve of real assets or funds, some of which being sponsored by large technology or financial firms with a large customer base. The report underlines that "stablecoins" that have the potential to reach a global scale (the so-called "global stablecoins") are likely to raise additional challenges in terms of financial stability, monetary policy transmission and monetary sovereignty, among others. Users of "stablecoins" could in principle be exposed, among others, to liquidity risk (it may take time to cash in such a "stablecoin"), counterparty credit risk (issuer may default) and market risk (if assets held by issuer to back the "stablecoin" lose value).*

Question 12. In our view, what are the benefits of ‘stablecoins’ and ‘global stablecoins’?

Stablecoins issued by Central Banks is, in our view, only a matter of time. We firmly believe that this type of 'funds' will be issued by Central Banks in the relatively near future (if not already done so currently in a testing phase). (Global) stablecoins would, naturally, be very interesting from an Fx risk perspective. It would have huge impact on Fx risks as well as on derivatives markets, making cross border business operations and trading etc. much cheaper for many businesses.

Stablecoins issued by others than Central Banks, and in particular global stablecoins, should be subject to stringent capital requirements in order to make sure that the stablecoins are really stable and that (other than general money devaluation risks) the stablecoin is really similar to the (fiat) currency to which the stablecoin is pegged.

Question 13. In your opinion, what are the most important risks related to “stablecoins”?

	1 (factor not relevant at all)	2	3	4	5 (very relevant factor)	Don’t know / no opinion / not relevant
Fraudulent activities	○	○	○	○	◉	○
Market integrity (e.g. price, volume manipulation...)	○	○	○	○	◉	○
Investor/consumer protection	○	○	○	○	◉	○
Anti-money laundering and CFT issues	○	○	○	◉	○	○
Data protection issues	○	○	◉	○	○	○
Competition issues	○	○	◉	○	○	○
Cyber security and operational risks	○	○	○	◉	○	○
Taxation issues	○	○	◉	○	○	○
Energy consumption	○	○	◉	○	○	○
Financial stability	○	○	○	○	◉	○
Monetary sovereignty/monetary policy transmission	○	○	○	○	◉	○

Some EU Member States already regulate crypto-assets that fall outside the EU financial services legislation. The following questions seek views from stakeholders to determine whether a bespoke regime on crypto-assets at EU level could be conducive to a thriving crypto-asset market in Europe and on how to frame a proportionate and balanced regulatory framework, in order support legal certainty and thus innovation while reducing the related key risks. To reap the full benefits of crypto-assets, additional modifications of national legislation may be needed to ensure, for instance, the enforceability of token transfers.

Question 14. In your view, would a bespoke regime for crypto-assets (that are not currently covered by EU financial services legislation) enable a sustainable crypto-asset ecosystem in the EU (that could otherwise not emerge)?

Yes. By its nature, crypto assets can easily transfer from one to another. With reference to the CMU plans and the FinTech Action Plan on the basis thereof, crypto-assets could well be a manner in which SMEs can attract alternative financing as well as offering (Retail) investors a possibility to invest their funds in a relatively easy manner. Potentially, the crypto asset market can be very interesting for both types of stakeholders. However, it is very important that the relevant interests of both sides are taken into account in the legal framework applicable to it. On the on hand, investors need to be well informed and if needed be protected against themselves by not making available an investment opportunity to retail investors in respect of specific types of crypto assets or derivatives based on crypto assets. Also, offering an exit possibility to investors (e.g. by making the crypto asset transferable/tradable/redeemable/interchangeable/etc.) is, in our view, important to take into account when thinking about a regulatory framework, as it is generally in the interest of (retail) investors to be able to make their investments liquid if they need the funds for something else. On the other hand, offering SMEs this source to alternative financing whilst ensuring that they inform their investors in an adequate, complete, not-misleading manner in a similar way (and to that end tech-neutral) as other companies that, for example, offer securities in compliance with the Prospectus Regulation, if also very important. In order to prevent regulatory arbitrage and, perhaps more importantly, to prevent a complex, scattered regulatory framework which differs in every Member State, in our view it is important that a framework will be developed on a EU-level. The (draft) Crowdfunding Regulation could perhaps function as a basis, offering a more proportionate framework for so called crowdfunding services providers on the basis of a 'light MiFID' regime including passporting possibilities to the crowdfunding service providers as well as the possibility for investors to transfer the 'crowdfunding assets' via a bulletin board (without the crowdfunding service provider immediately being required to obtain a regular MiFID II license for operating a trading venue such as an MTF). Perhaps a similar approach can be examined for 'crypto services providers'. In a (Delegated) Regulation, specific operating rules should be applicable to prevent/minimize cyber risks and to clarify liabilities in the event of, for example, hacks, wrongly programmed algorithms underlying the crypto assets (including tokens with smart contract functionalities), etc. Also, specific guidelines should be applicable as to the type of blockchain to be used (open/public/permissioned/permissionless, use of oracles, rights of regulatory authorities, etc), whitelisting rules (incl. AMLD V but one can also think of selling and transfer restrictions embedded/programmed into the crypto assets to prevent the possibility for a crypto asset to be offered to and/or transferred outside the EEA for example).On a separate note, AMLD V obligations are of such great importance in order for the crypto asset market to develop in a prudent and crypto assets to develop into a well accepted asset class. In our view, the KYC/CDD obligations arising from AMLD V should be applicable to any type of crypto asset provider acting in the course of its business or profession.

Question 15. What is your experience (if any) as regards national regimes on crypto-assets? Please indicate which measures in these national laws are, in your view, an effective approach to crypto-assets regulation, which ones rather not.

Other than the - expected - implementation of AMLD V in the Dutch AML Act, there is no specific Dutch law regime applicable to crypto assets (yet). The Dutch regulators, DNB and the AFM, did publish warnings to investors (comparable to many other financial regulators globally) and emphasized to issuers/companies and 'crypto asset service providers' that the current regulatory framework could be applicable to any crypto initiative taken or developed by any such stakeholder.

As legal advisors, we have advised in respect of multiple crypto asset initiatives and have been involved in multiple blockchain projects in which tokenization and smart contract functionalities play an important role. Some projects (including some ICO initiatives) clearly fell within the existing regulatory framework such as the Prospectus Regulation and related securities laws, AIFMD and MiFID II. Other projects were not as clear cut and some of those projects were discussed in depth with the relevant Dutch regulator.

The Dutch regulators are very much willing to accept trustworthy parties offering services on the basis of DLT and using tokenization as a means to make certain assets tradable in whole or in part (including tangible assets), but the fact that the current regulatory framework was not drawn up taking into account crypto assets (including smart contracts/tokens), we noticed the relative difficulty in obtaining the relevant authorizations or guidance from the Dutch regulators.

On paper, there is a regulatory sandbox initiative taken by the Dutch regulators, but our clients have not yet been able to be admitted to the sandbox. We are in huge favour of opening up a regulatory sandbox for FinTech initiatives, including those of crypto asset service providers. However, in our view, only Fintech companies (including crypto asset service providers) that are willing to comply with a minimum set of financial regulatory rules and AML/CFT rules (in particular KYC/CDD), information obligations and, to the extent relevant, some prudential safeguards (segregation of funds, perhaps limited capital requirement), should be offered access to the regulatory sandbox but should not, from the outset, need to comply in full with, for example, MiFID II, etc. A regulatory sandbox could be a useful tool for all stakeholders involved to learn real time in a monitored environment which is open to a limited number of investors/clients and where other safeguards can be included such as a maximum investment amount per investor etc until the company is ready for the next step and can expand its license/authorization as well as, simultaneously, the proportionality of the regulatory framework applicable to the size of its business, the number of its employees, its turnover, the number of transactions via/with the assistance of the FinTech company (/ crypto asset service provider), - to the extent relevant- the assets under management, and other growth/volume indicators.

Question 16. In your view, how would it be possible to ensure that a bespoke regime for crypto-assets and crypto-asset service providers is proportionate to induce innovation, while protecting users of crypto-assets? Please indicate if such a bespoke regime should include the above- mentioned categories (payment, investment and utility tokens) or exclude some of them, given their specific features (e.g. utility tokens).

We defer to our answers to questions 14 and 15 above. At this stage, we doubt whether there should be made a distinction between the different categories of crypto assets if and to the extent those crypto assets can be directly purchased by investors (whether in a primary market or secondary market). The rationale for this remark is that - other than for the issuer - it is practically impossible for crypto asset service providers such as exchanges to review each individual whitepaper to determine whether crypto asset A qualifies as a security, crypto asset B as a payment token, crypto asset C as a derivative, crypto asset D as a participation right in a collective investment scheme, crypto asset E as a stablecoin, and crypto asset F as merely a utility token which does not have any real time financial value as it only has a function within e.g. a virtual game (and where such utility token is similar to buying gaming playing 'credit' etc). As the type of crypto asset may result in a different regulatory framework to be applicable to their (intermediary) roles, in our view it may become very cumbersome for such (professional) intermediaries to determine the type of crypto asset and therefore the regulatory framework applicable to it. Moreover, if this is the responsibility of such crypto asset service providers themselves, chances are high that there will be deviating classifications made by different crypto asset services providers, resulting in arbitrage risks and differences in regulatory safeguards put around a particular crypto asset depending on the crypto asset service provider being involved, both unintended and intended. Moreover, what we have seen happening in the past, is that certain crypto assets have developed in another category overtime, or were hybrid forms of crypto assets from the outset. How to deal with that? In our view it cannot be that the regulatory framework applicable to a crypto asset changes over time due to the manner in which such crypto assets is used or received by investors/its users. All parties involved need to be offered legal certainty. Lastly, in our view it could be very difficult, taking into account the continuous development of technology and the ongoing development of innovative use cases and appearances, to formulate a regulatory framework applicable to crypto assets in which such a distinction is made. Soon there will be new types of crypto assets created, resulting again in ambiguity and potential arbitrage as to the regulatory framework applicable to such a new type of crypto asset.

B. Specific questions on service providers related to crypto-assets

The crypto-asset market encompasses a range of activities and different market actors that provide trading and/or intermediation services. Currently, many of these activities and service providers are not subject to any regulatory framework, either at EU level (except for AML/CFT purposes) or national level. Regulation may be necessary in order to provide clear conditions governing the provisions of these services and address the related risks in an effective and proportionate manner. This would enable the development of a sustainable crypto-asset framework. This could be done by bringing these activities and service providers in the regulated space by creating a new bespoke regulatory approach.

Question 19. Can you indicate the various types and the number of service providers related to crypto-assets (issuances of crypto-assets, exchanges, trading platforms, wallet providers, ...) in your jurisdiction?

We defer to the report of the Dutch regulators dated January 2019 (https://www.afm.nl/en/nieuws/2019/jan/adviesrapport-crypto). The different types of crypto asset service providers are well described in the annex to that report. We do not have a clear view on the number of the different crypto asset service providers in the Netherlands (other than our own clients).

1. Issuance of crypto-assets

This section distinguishes between the issuers of crypto-assets in general (1.1.) and the issuer of the so-called "stablecoins" backed by a reserve of real assets (1.2.).

1.1. Issuance of crypto-assets in general

The crypto-asset issuer or sponsor is the organisation that has typically developed the technical specifications of a crypto-asset and set its features. In some cases, their identity is known, while in some cases, those promoters are unidentified. Some remain involved in maintaining and improving the crypto-asset's code and underlying algorithm while other do not (study from the European Parliament on "Cryptocurrencies and Blockchain", July 2018). Furthermore, the issuance of crypto-assets is generally accompanied with a document describing crypto-asset and the ecosystem around it, the so-called 'white papers'. Those 'white papers' are, however, not standardised and the quality, the transparency and disclosure of risks vary greatly. It is therefore uncertain whether investors or consumers who buy crypto-assets understand the nature of the crypto-assets, the rights associated with them and the risks they present.

Question 20. Do you consider that the issuer or sponsor of crypto-assets marketed to EU investors/consumers should be established or have a physical presence in the EU?

No. We do hold the view that such issuers/sponsors should be established somewhere in the world and that the Dutch (/EU) marketing rules shall be complied with when such crypto assets are offered to the public in the Netherlands (EU), but we do not see a reason why the crypto asset primary market within the EEA should be limited to companies established in a member state of the EEA; issuers of securities established in a third country can currently also offer securities to the public in the Netherlands/EEA subject to the Prospectus Regulation. Why should an offer of crypto asset be treated differently from this respect, in particular now blockchain/DLT enables such an issuer/sponsor to easily offer such crypto assets in other jurisdictions?

Question 21. Should an issuer or a sponsor of crypto-assets be required to provide information (e.g. through a 'white paper') when issuing crypto-assets? Please indicate the entity that, in your view, should be responsible for this disclosure (e.g. the issuer/sponsor, the entity placing the crypto-assets in the market) and the content of such information (e.g. information on the crypto-asset issuer, the project, the rights attached to the crypto-assets, on the secondary trading, the underlying technology, potential conflicts of interest, ...).

Yes. In our view, the current regulatory framework applicable to securities (Prospectus Regulation), units in a collective investment scheme (Prospectus Regulation or AIFMD), PRIIPs and the national civil law marketing rules etc. could form an example of the information requirements that should be followed in respect of crypto assets. Although we do not quite favour yet another type of 'key information document', presumably another standardized 'KID' needs to be developed for crypto assets taken their peculiarities and the relevance of technology for the functionality of such crypto assets. In our view the issuer should be primarily responsible for compliance with information requirements. We do hold the view that intermediary parties offering their services in the course of their business or profession and therefore can be considered (more) professional, do have a duty of care towards their clients as well. They will, presumably, not be in the position to draft a whitepaper or standardized information document, but we could imagine a role for them as well in a placement process or alike services comparable to the role of placement agents/underwriters under MiFID II and the Prospectus Regulation (e.g. consent requirement under Prospectus Regulation, ensuring that their clients, the investors, have received the whitepaper, whether the investment opportunity is in line with the investor's profile and risk appetite, etc). Retail investors should simply be warned that they should not invest in crypto assets directly prior to having obtained professional advice if they do not understand the risks involved.

Question 22. If a requirement to provide the information on the offers of crypto-assets is imposed on their issuer/sponsor, would you see a need to clarify the interaction with existing pieces of legislation that lay down information requirements (to the extent that those rules apply to the offers of certain crypto-assets, such as utility and/or payment tokens)?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
The Consumer Rights Directive	○	○	○	○	◉	○
The E-Commerce Directive	○	○	○	◉	○	○
The EU Distance Marketing of Consumer Financial Services Directive	○	○	○	○	◉	○

Reasoning: We are not sure whether these pieces of legislation would actually need to be clarified; presumably they would all need to be complied with in respect of the offering of services in respect of crypto assets.

22.1 Is there any other existing piece of legislation laying down information requirements with which the interaction would need to be clarified? Please specify which one(s) and explain your reasoning:

Prospectus Regulation, AIFMD, PRIIPs, [Crowdfunding Regulation]. For our reasoning we kindly defer you to our prior answers.

Further, perhaps the Unfair Commercial Practices Directive (2005/29/EC), the Directive concerning misleading and comparative advertising (2006/114/EC) and the Unfair Contracts Terms Directive (93/13/EEC).

Question 23. Beyond any potential obligation as regards the mandatory incorporation and the disclosure of information on the offer, should the crypto-asset issuer or sponsor be subject to other requirements?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
The managers of the issuer or sponsor should be subject to fitness and probity standards	○	○	○	○	◉	○
The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions	○	○	○	○	◉	○
Where necessary, the issuer or sponsor should put in place a mechanism to safeguard the funds collected such as an escrow account or trust account	○	○	○	○	◉	○

1.2. Issuance of “stablecoins” backed by real assets

As indicated above, a new subset of crypto-assets – the so-called “stablecoins” – has recently emerged and present some opportunities in terms of cheap, faster and more efficient payments. A recent G7 report makes a distinction between “stablecoins” and “global stablecoins”. While “stablecoins” share many features of crypto-assets, the so-called “global stablecoins” (built on existing large and cross-border customer base) could scale rapidly, which could lead to additional risks in terms of financial stability, monetary policy transmission and monetary sovereignty. As a consequence, this section of the public consultation aims to determine whether additional requirements should be imposed on both “stablecoin” and “global stablecoin” issuers when their coins are backed by real assets or funds. The reserve (i.e. the pool of assets put aside by the issuer to stabilise the value of a “stablecoin”) may be subject to risks. For instance, the funds of the reserve may be invested in assets that may prove to be riskier or less liquid than expected in stressed market circumstances. If the number of “stablecoins” is issued above the funds held in the reserve, this could lead to a run (a large number of users converting their “stablecoins” into fiat currency).

Question 24. In your opinion, what would be the objective criteria allowing for a distinction between “stablecoins” and “global stablecoins” (e.g. number and value of “stablecoins” in circulation, size of the reserve, ...)? Please explain your reasoning.

With reference to our answer to question 12, we do see the benefits of (global) stablecoins, subject to these really being pegged against assets of the same, stable, value. Stablecoins could be less volatile than other types of crypto assets, as they would, presumably, follow the curves/trends of the underlying asset.

However, global stablecoins upon issuance (such as potentially the Libra) could have huge impact and raise incredible financial stability risks if not properly managed. Any issuers of such stablecoins should, in our view, be subject to similar capital requirements as credit institutions depending on the systemic risk they bring along in terms of 'AuM'. Moreover, it should be given thought whether any (fiat) assets paid in exchange for such global stablecoin should be considered a deposit within the meaning of the DGSD.

Any stablecoin issued on a public permissionless blockchain could, in theory, become a global stablecoin though. In line with our prior responses, we are in favour of a regulatory framework the requirements of which grow with the undertaking falling under the scope of the regulatory framework. Start would be a registration or license requirement ensuring the issuer of such stablecoin meets certain minimum requirements, including some capital requirements and segregation of funds requirements. Depending on volume indicators, the undertaking would need to upgrade its license and would become subject to a more stringent regulatory framework. Number of clients, value of stablecoins issued/pegged assets, volume of transactions, turnover, etc. could all be indicators that the issuer of the stablecoins needs to top up its license (within a certain time frame following such indicator being met and for example on an annual basis including the requirement to issue a negative statement to the NCA to inform the NCA if no volume indicator requires the issuer to top up its license).

Question 25. To tackle the specific risks created by "stablecoins" and "global stablecoins", what are the requirements that could be imposed on their issuers and/or the manager of the reserve?

	Relevant	Not relevant	Don't know / no opinion
The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)	◉	○	○
The issuer should contain the creation of "stablecoins" so that it is always lower or equal to the value of the funds of the reserve	◉	○	○
The assets or funds of the reserve should be segregated from the issuer's balance sheet	◉	○	○
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	○	○	◉
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	◉	○	○
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	◉	○	○
Obligation for the assets or funds to be held in custody with credit institutions in the EU	○	◉	○
Periodic independent auditing of the assets or funds held in the reserve	◉	○	○
The issuer should disclose information to the users on (i) how it intends to provide stability to the "stablecoins", (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve	◉	○	○
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	◉	○	○
Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer	◉	○	○

Reasoning: We limit our response to the statements where we have not indicated these to be relevant to stablecoins.

As regards the statement that 'the assets of the reserve should not be encumbered (i.e. not pledged as collateral)', we feel that there could be a distinction made if these assets are pledged to the ECB to obtain credit from the ECB in line with the current lending possibilities for credit institutions.

As regards the statement that there should be an 'obligation for the assets or funds to be held in custody with credit institutions in the EU', we hold the view that it would be much better if these assets or funds would be held in custody directly with the national central bank or the ECB. This limits a potential systemic risk due to the credit institution involved.

Unless credit institutions will be subjected to specific capital requirements in respect of any such reserve assets of a stablecoin issuer (which we are not in favour of because in that case stablecoins will presumably become quite expensive for customers), such credit institutions involved will use those funds to finance loans provided at the risk and account of such credit institution. A run on a stablecoin issuer upon stablecoin holders requesting redemption of their stablecoins in fiat currency or other underlying asset, may also result in the credit institution involved to get into liquidity problems (naturally depending on the reserve and as such number of issued stablecoins). As disclosure of the underlying assets and manner of segregation of funds is important, a run on the stablecoin issuer could result in a bankrun on that specific credit institution involved, which in turn can have further systemic risks.

In addition to the above, we favour a more competitive landscape. If stablecoin providers are dependent on credit institutions to be able to comply with segregation requirements (like PSPs are currently are dependent on credit institutions for settling payment transactions within the TARGET2 framework), credit institutions have a monopolist role in this type of innovation. We prefer a competitive landscape, yet with the relevant regulatory framework applicable to such stablecoin providers (including capital requirements).

25.1) Is there any other requirements not mentioned above that could be imposed on “stablecoins” issuers and/or the manager of the reserve?.

A stablecoin would (in our view) generally qualify as a derivative and it would qualify as an electronic money within the meaning of EMD2 and therefore as a type of fund within the meaning of PSD2. All the relevant EU legislation in this regard, such as PSD2, EMD2, EMIR / EMIR Refit and MiFID II/MiFIR, should be reviewed in relation to its relevance to the issuance of stablecoins. As mentioned above in answer 24, we also give in consideration to determine whether DGSD should be applicable to stablecoins.

“Stablecoins” could be used by anyone (retail or general purpose) or only by a limited set of actors, i.e. financial institutions or selected clients of financial institutions (wholesale). The scope of uptake may give rise to different risks. The G7 report on “investigating the impact of global stablecoins” stresses that “Retail stablecoins, given their public nature, likely use for high-volume, small-value payments and potentially high adoption rate, may give rise to different risks than wholesale stablecoins available to a restricted group of users”.

Question 26. Do you consider that wholesale “stablecoins” (those limited to financial institutions or selected clients of financial institutions, as opposed to retail investors or consumers) should receive a different regulatory treatment than retail “stablecoins”?

Yes. Wholesale 'investors' can, comparable to professional investors/eligible counterparties within the meaning of MIFID II, be considered to better understand the risks involved etc.

2. Trading platforms

Trading platforms function as a market place bringing together different crypto-asset users that are either looking to buy or sell crypto-assets. Trading platforms match buyers and sellers directly or through an intermediary. The business model, the range of services offered and the level of sophistication vary across platforms. 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 platform (off-chain) in the case of centralised platforms, while it occurs on DLT for decentralised platforms (on-chain). Some platforms have already adopted good practice from traditional securities trading venues19 while others use simple and inexpensive technology.

[19] Trading venues are a regulated market, a multilateral trading facility or an organised trading facility under MiFID II

Question 27. In your opinion and beyond market integrity risks (see section III. C. 1. below), what are the main risks in relation to trading platforms of crypto-assets?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Absence of accountable entity in the EU	○	◉	○	○	○	○
Lack of adequate governance arrangements, including operational resilience and ICT security	○	○	○	○	◉	○
Absence or inadequate segregation of assets held on the behalf of clients (e.g. for 'centralised platforms')	○	○	○	○	◉	○
Conflicts of interest arising from other activities	○	○	○	◉	○	○
Absence/inadequate recordkeeping of transactions	○	○	○	○	◉	○
Absence/inadequate complaints or redress procedures are in place	○	○	◉	○	○	○
Bankruptcy of the trading platform	○	○	○	◉	○	○
Lacks of resources to effectively conduct its activities	○	○	○	◉	○	○

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Losses of users' crypto-assets through theft or hacking (cyber risks)	○	○	○	○	◉	○
Lack of procedures to ensure fair and orderly trading	○	○	○	◉	○	○
Access to the trading platform is not provided in an undiscriminating way	○	○	◉	○	○	○
Delays in the processing of transactions	○	○	○	○	◉	○
For centralised platforms: Transaction settlement happens in the book of the platform and not necessarily recorded on DLT. In those cases, confirmation that the transfer of ownership is complete lies with the platform only (counterparty risk for investors vis-à-vis the platform)	○	○	○	◉	○	○
Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse	○	○	○	○	◉	○

Reasoning: with reference to our prior answers, we find it important that crypto assets can be traded between holders. However, if a full MiFID II regime becomes applicable to 'crypto asset trading service providers' that have their seats in the EEA, this may be too burdensome for any new operator to offer such trading services.

Taken the cross border trading possibilities by nature of crypto assets, it should also be carefully considered how it can be guaranteed that trading on a platform by any crypto asset holder residing in the EEA does not violate any applicable local rules (in particular in the US and jurisdictions where ICOs and trading in crypto assets is prohibited in full).

Question 28. What are the requirements that could be imposed on trading platforms in order to mitigate those risks?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Trading platforms should have a physical presence in the EU	○	○	○	◉	○	○
Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)	○	○	○	○	◉	○
Trading platforms should segregate the assets of users from those held on own account	○	○	○	○	◉	○
Trading platforms should be subject to rules on conflicts of interest	○	○	◉	○	○	○
Trading platforms should be required to keep appropriate records of users' transactions	○	◉	○	○	○	○
Trading platforms should have an adequate complaints handling and redress procedures	○	○	◉	○	○	○
Trading platforms should be subject to prudential requirements (including capital requirements)	○	○	○	◉	○	○
Trading platforms should have adequate rules to ensure fair and orderly trading	○	○	○	◉	○	○
Trading platforms should provide access to its services in an undiscriminating way	○	○	○	◉	○	○
Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse	○	○	○	○	◉	○
Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)	○	◉	○	○	○	○
Trading platforms should be responsible for screening crypto-assets against the risk of fraud	○	○	○	◉	○	○

28.1 Is there any other requirement that could be imposed on trading platforms in order to mitigate those risks? Please specify which one(s) and explain your reasoning:

Not on trading platforms itself, but in our view it could be very beneficial - if the trading venue is run on a blockchain itself - to offer the NCAs rights to the blockchain to view and extract the trading data directly from the blockchain for transaction reporting and monitoring purposes and to run those data against AML/CFT/MAR algo's and databases.

28.2 Please indicate if those requirements should be different depending on the type of crypto-assets traded on the platform and explain your reasoning for your answers to question 28:

Our answers to question 28 are based on the presumption that the trading platform will run on DLT itself and that the NCAs will have rights to the blockchain, making it less important to subject trading platforms to (separate) reporting requirements and record-holding. The latter does not make sense if DLT is used; all nodes will have a copy of the register and should function as a transparent register. Subjecting the platform to a parallel administration requirement detracts from the functionalities and added value of DLT.

3. Exchanges (fiat-to-crypto and crypto-to-crypto)

Crypto-asset exchanges are entities that offer exchange services to crypto-asset users, usually against payment of a certain fee (i.e. a commission). By providing broker/dealer services, they allow users to sell their crypto-assets for fiat currency or buy new crypto-assets with fiat currency. It is important to note that some exchanges are pure crypto-to-crypto exchanges, which means that they only accept payments in other crypto-assets (for instance, Bitcoin). It should also be noted that many cryptocurrency exchanges (i.e. both fiat-to-crypto and crypto-to-crypto exchanges) operate as custodial wallet providers (see section III.B.4 below). Many exchanges usually function both as a trading platform and as a form of exchange (study from the European Parliament on "Cryptocurrencies and Blockchain", July 2018).

Question 29. In your opinion, what are the main risks in relation to crypto-to-crypto and fiat–to-crypto exchanges?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Absence of accountable entity in the EU	○	○	◉	○	○	○
Lack of adequate governance arrangements, including operational resilience and ICT security	○	○	○	○	◉	○
Conflicts of interest arising from other activities	○	○	○	◉	○	○
Absence/inadequate recordkeeping of transactions	○	◉	○	○	○	○
Absence/inadequate complaints or redress procedures are in place	○	○	◉	○	○	○
Bankruptcy of the exchange	○	○	○	○	◉	○
Inadequate own funds to repay the consumers	○	○	○	○	◉	○
Losses of users' crypto-assets through theft or hacking	○	○	○	○	◉	○
Users suffer loss when the exchange they interact with does not exchange crypto-assets against fiat currency (conversion risk)	○	○	○	◉	○	○
Absence of transparent information on the crypto-assets proposed for exchange	○	○	○	◉	○	○

Reasoning: This assessment of risks involved depend on the manner in which trading takes place (on chain or off chain). On chain trading gives more transparency and less counterparty risk in our view.

29.1 Is there any other main risks in relation to crypto-to-crypto and fiat–to-crypto exchanges not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning:

AML/CFT risks in relation to exchanges offering crypto-to-crypto services. In the draft Dutch bill implementing AMLD V in the Dutch AML Act, only exchanges offering exchange services from fiat-to-crypto and vice versa are brought under the scope of the Dutch AML Act. In line with the FATF recommendations, we are in favour of subjecting exchanges offering crypto-to-crypto services to AML/CFT requirements as well.

Question 30. What are the requirements that could be imposed on exchanges in order to mitigate those risks?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Absence of accountable entity in the EU	○	○	◉	○	○	○
Exchanges should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)	○	○	○	○	◉	○
Exchanges should segregate the assets of users from those held on own account	○	○	○	○	◉	○
Exchanges should be subject to rules on conflicts of interest	○	○	○	◉	○	○
Exchanges should be required to keep appropriate records of users' transactions	○	◉	○	○	○	○
Exchanges should have an adequate complaints handling and redress procedures	○	○	◉	○	○	○
Exchanges should be subject to prudential requirements (including capital requirements)	○	○	○	○	◉	○
Exchanges should be subject to advertising rules to avoid misleading marketing/promotions	○	○	○	○	◉	○
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)	○	◉	○	○	○	○

Exchanges should be responsible for screening crypto-assets against the risk of fraud	○	○	○	○	○	◉

Reasoning: making platform responsible for screening against the risk of fraud is a bridge too far in our view. It would be a responsibility that is almost impossible to comply with in the event of actual fraud. However, certain due diligence requirements and perhaps certain best effort obligations to verify identity of issuer (in line with AML/CFT requirements) and use of proceeds of offering of crypto assets could be useful to protect the interests of investors in such crypto assets. However, fraudulent schemes cannot be prevented in full (not by a crypto assets trading platform; nor by an operator of a regulated market/MTF/OTF).

4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys[20] and to interact with DLT 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[21]. DLT networks generally provide their own wallet functions (e.g. Bitcoin or Ether).

There are also specialised 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. They can also provide an overview of the customers' transactions. Different risks can arise from the provision of such a service.

[20] *DLT is built upon a cryptography 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] *There are software/hardware wallets and so-called cold/hot wallets. A software wallet is an application that may be installed locally (on a computer or a smart phone) or run in the cloud. A hardware wallet is a physical device, such as a USB key. Hot wallets are connected to the internet while cold wallets are not.*

Question 31. In your opinion, what are the main risks in relation to the custodial wallet service provision?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
No physical presence in the EU	○	○	◉	○	○	○
Lack of adequate governance arrangements, including operational resilience and ICT security	○	○	○	○	◉	○
Absence or inadequate segregation of assets held on the behalf of clients	○	○	○	○	◉	○
Conflicts of interest arising from other activities (trading, exchange)	○	○	○	○	◉	○
Absence/inadequate recordkeeping of holdings and transactions made on behalf of users	○	◉	○	○	○	○
Absence/inadequate complaints or redress procedures are in place	○	○	○	◉	○	○
Bankruptcy of the custodial wallet provider	○	○	○	○	◉	○

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Inadequate own funds to repay the consumers	○	○	○	○	◉	○
Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)	○	○	○	○	◉	○
The custodial wallet is compromised or fails to provide expected functionality	○	○	○	○	◉	○
The custodial wallet provider behaves negligently or fraudulently	○	○	○	○	◉	○
No contractual binding terms and provisions with the user who holds the wallet	○	○	○	○	◉	○

Reasoning: It is of the essence that custodial wallet providers - who hold (a copy of) private keys of their clients - make sure that those private keys are deposited with/held by them in a safe manner and that they can function as a trusted third party like other custodians currently do in respect of other assets such as financial instruments (in book-entry form, registered or in bearer form). Similar rules as applicable to custodians, asset managers and, potentially, CSDs could become applicable to custodial wallet providers if the crypto assets in respect of which they hold the private keys qualify as financial instruments within the meaning of MiFID II

We do note that in our view the use of crypto assets by a company for merely back end reasons in order to have its back end administration benefit from the functionalities and advantages of DLT should be treated differently. It could be that due to a back end system of a company running on DLT, the company 'converts' the financial product offered on its platform into crypto assets and holds the private keys of such 'internally used crypto assets' on behalf of the users of its platform. Such 'back end custodial wallet providers' should be treated differently as the front end clients will not necessarily be prejudiced by these risks materializing as they may still have the original, actual, front end, rights irrespective of a private key being stolen etc. This would more be an administrative and evidence issue rather than a legal/ownership issue.

Question 32. What are the requirements that could be imposed on custodial wallet providers in order to mitigate those risks?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Custodial wallet providers should have a physical presence in the EU	○	○	◉	○	○	○
Custodial wallet providers should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)	○	○	○	○	◉	○
Custodial wallet providers should segregate the asset of users from those held on own account	○	○	○	○	◉	○
Custodial wallet providers should be subject to rules on conflicts of interest	○	○	○	○	◉	○
Custodial wallet providers should be required to keep appropriate records of users' holdings and transactions	○	◉	○	○	○	○
Custodial wallet providers should have an adequate complaints handling and redress procedures	○	○	◉	○	○	○
Custodial wallet providers should be subject to capital requirements	○	○	○	◉	○	○
Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions	○	○	○	◉	○	○
Custodial wallet providers should be subject to certain minimum conditions for their contractual relationship with the consumers/investors	○	○	○	◉	○	○

Question 33. Should custodial wallet providers be authorised to ensure the custody of all crypto-assets, including those that qualify as financial instruments under MiFID II (the so-called 'security tokens', see section IV of the public consultation) and those currently falling outside the scope of EU legislation?

Yes. As mentioned before, in our view, only a very limited number of crypto assets would (or should) not qualify as financial instruments within MiFID II or fall outside the scope of a regulatory framework. We do not see any reason why custodial wallet providers, if subjected to an appropriate regulatory framework, should not be able to offer custody services for all types of crypto assets.

5. Other services providers

Beyond custodial wallet providers, exchanges and trading platforms, other actors play a particular role in the crypto- asset ecosystem. Some bespoke national regimes on crypto-currency regulate (either on an optional or mandatory basis) other crypto-assets related services, sometimes taking examples of the investment services listed in Annex I of MiFID II. The following section aims at assessing whether some requirements should be required for other services.

Question 35. In your view, what are the services related to crypto-assets that should be subject to requirements? (When referring to execution of orders on behalf of clients, portfolio management, investment advice, underwriting on a firm commitment basis, placing on a firm commitment basis, placing without firm commitment basis, we consider services that are similar to those regulated by Annex I A of MiFID II.)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Reception and transmission of orders in relation to crypto-assets	○	○	○	○	◉	○
Execution of orders on crypto-assets on behalf of clients	○	○	○	○	◉	○
Crypto-assets portfolio management	○	○	○	○	◉	○
Advice on the acquisition of crypto-assets	○	○	○	○	◉	○
Underwriting of crypto-assets on a firm commitment basis	○	○	○	○	◉	○
Placing crypto-assets on a firm commitment basis	○	○	○	○	◉	○
Placing crypto-assets without a firm commitment basis	○	○	○	○	◉	○

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)	○	○	◉	○	○	○
Processing services, also known as 'mining' or 'validating' services in a DLT environment (e.g. 'miners' or validating 'nodes' constantly work on verifying and confirming transactions)	○	○	◉	○	○	○
Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)	○	○	○	◉	○	○
Services provided by developers that are responsible for maintaining/updating the underlying protocol	○	○	◉	○	○	○
Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)	○	○	◉	○	○	○

Reasoning: The severity of applicable requirements depends in our view on several factors, such as the type of blockchain used, the consensus protocol of the blockchain and corresponding level of interdependencies, etc. The more robust the blockchain is, the lower certain requirements can be in our view thanks to the nature of this technology.

Generally, we hold the view that as long as any services would fall within the scope of existing EU legislation such as MiFID II if the crypto assets qualify as financial instruments (or any other financial product, such as a fund within the meaning of PSD2 and/or electronic money within the meaning of EMD2), that such a service provider should fall under a regulatory framework. With reference to our prior answers, we, however, favour a 'base authorisation/license requirement' which offers the right balance between investor protection, financial stability, market integrity and proportionality for the crypto asset provider involved and which authorisation regime (and severity of requirements) grows with the undertaking on the basis of appropriate volume indicators. We favour this approach not just in relation to crypto asset providers but to any FinTech company or other start-up company offering financial services.

35.1 Is there any other services related to crypto-assets not mentioned above that should be subject to requirements? Please specify which one(s) and explain your reasoning:

- Responsibility for developing/programming algorithm(s) in respect of the crypto-asset;
- Responsibility for ensuring accurate, complete and not-misleading information provision to investors (and appropriate 'translation' of programming language compared to comprehensible information provided to (retail) investor.

Crypto-assets are not banknotes, coins or scriptural money. For this reason, crypto-assets do not fall within the definition of 'funds' set out in the Payment Services Directive (PSD2), unless they qualify as electronic money. As a consequence, if a firm proposes a payment service related to a crypto-asset (that do not qualify as e-money), it would fall outside the scope of PSD2.

Question 36. Should the activity of making payment transactions with crypto-assets (those which do not qualify as e-money) be subject to the same or equivalent rules as those currently contained in PSD2?

This is a tricky one. At this stage, crypto assets seem to be too volatile to function as a fund within the meaning of PSD2 and it could be argued that payments made in crypto assets come to the full risk of the parties involved in such payment transaction. If one prefers to be paid by other means than 'PSD2 funds' for whatever reason, it is his choice and he may be deemed to accept the risks involved. However, the question is whether everyone is aware of such risks and whether they should not be better protected against such risks (and against their own ignorance). While the crypto asset payment market may still be relatively small and immature, this could develop quickly, especially if any BigTech would offer such payment services (if not already done so). To that end, the mere fact that crypto assets currently legally do not qualify as 'PSD2 funds' (excluding potential electronic money equivalents) should not prevent PSD2 (and alike legislation) from being applicable. We note that clarity in respect of the regulatory approach of crypto assets, could also result in clarity in respect of the civil law and tax law approaches of crypto assets (e.g. can crypto assets be pledged?; Can a creditor take recourse against crypto assets of its debtor? Can a custodial wallet provider be served with a garnishee order in respect of crypto assets held in its custody?).

C. Horizontal questions

Those horizontal questions relate to four different topics: Market integrity (1.), AML/CFT (2.), consumer protection (3.) and the supervision and oversight of the various service providers related to crypto-assets (4).

1. Market Integrity

Many crypto-assets exhibit high price and volume volatility while lacking the transparency and supervision and oversight present in other financial markets. This may heighten the potential risk of market manipulation and insider dealing on exchanges and trading platforms. These issues can be further exacerbated by trading platforms not having adequate systems and controls to ensure fair and orderly trading and protect against market manipulation and insider dealing. Finally there may be a lack of information about the identity of participants and their trading activity in some crypto-assets.

Question 37. In your opinion, what are the biggest market integrity risks related to the trading of crypto-assets?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Price manipulation	○	○	○	◉	○	○
Volume manipulation (wash trades…)	○	○	○	○	○	◉
Pump and dump schemes	○	○	○	◉	○	○
Manipulation on basis of quoting and cancellations	○	○	○	○	○	◉
Dissemination of misleading information by the crypto-asset issuer or any other market participants	○	○	○	○	◉	○
Insider dealings	○	○	○	○	◉	○

Reasoning: On chain trading should be highly transparent and should limit market integrity risks to a great extent, subject to any trading investor being adequately identified and on boarded by the trading platform. Off chain trading is less transparent but could perhaps be better controlled by a trading platform. It should be prevented that any a-typical trading behaviour which could trigger MAR alarm bells to ring on other trading venues can be performed on crypto asset trading platforms without anyone noticing.

While market integrity is the key foundation to create consumers' confidence in the crypto-assets market, the extension of the Market Abuse Regulation (MAR) requirements to the crypto-asset ecosystem could unduly restrict the development of this sector.

Question 38. In your view, how should market integrity on crypto-asset markets be ensured?

With reference to prior answers: stimulate on chain trading by 'whitelisted' investors (being to the bare minimum investors identified in accordance with AML/CFT/KYC/CDD obligations), grant viewing/extraction rights to NCAs for transaction reporting/monitoring/MAR reasons, develop algorithms or other automatic data analysis tools that run on the trading platform on a continuous basis minimizing market integrity risks as much as possible.

While the information on executed transactions and/or current balance of wallets are often openly accessible in distributed ledger based crypto-assets, there is currently no binding requirement at EU level that would allow EU supervisors to directly identify the transacting counterparties (i.e. the identity of the legal or natural person(s) who engaged in the transaction).

Question 39. Do you see the need for supervisors to be able to formally identify the parties to transactions in crypto-assets?

Yes. We defer to our answer to question 38.

Question 40. Provided that there are new legislative requirements to ensure the proper identification of transacting parties in crypto-assets, how can it be ensured that these requirements are not circumvented by trading on platforms/exchanges in third countries?

Crypto assets may need a global approach rather than just a EU (or national) approach.

2. Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT)

Under the current EU anti-money laundering and countering the financing of terrorism (AML/CFT) legal framework (Anti-Money Laundering Directive (Directive 2015/849/EU) as amended by AMLD5 (Directive 2018/843/EU)), providers of services (wallet providers and crypto-to-fiat exchanges) related to "virtual currency" are "obliged entities". A virtual currency is defined as: "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically". The Financial Action Task Force (FATF) uses a broader term "virtual asset" and defines it as: "a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations". Therefore, there may be a need to align the definition used in the EU AML/CFT framework with the FATF recommendation or with a "crypto-asset" definition, especially if a crypto-asset framework was needed.

Question 41. Do you consider it appropriate to extend the existing "virtual currency" definition in the EU AML/CFT legal framework in order to align it with a broader definition (as the one provided by the FATF or as the definition of "crypto-assets" that could be used in a potential bespoke regulation on crypto-assets)?

Yes, we do consider it appropriate to extend the existing ''virtual currency'' definition in the EU AML/CFT legal framework in order to align with a broader definition. We defer to our answer to prior questions in which we already referred to the FATF recommendations and our recommendation to follow that definition/broader scope. In particular, crypto-to-crypto service providers should also fall under the scope of the AML/CFT legal framework in our view.

Some crypto-asset services are currently covered in internationally recognised recommendations without being covered under EU law, such as the provisions of exchange services between different types of crypto-assets (crypto-to-crypto exchanges) or the "participation in and provision of financial services related to an issuer"s offer and/or sale of virtual assets". In addition, possible gaps may exist with regard to peer-to-peer transactions between private persons not acting as a business, in particular when done through wallets that are not hosted by custodial wallet providers.

Question 42. Beyond fiat-to-crypto exchanges and wallet providers that are currently covered by the EU AML/CFT framework, are there crypto-asset services that should also be added to the EU AML/CFT legal framework obligations?

Yes. We do believe that there are crypto-asset services that should be added to the EU AML/CFT legal framework obligations. We defer to our prior answers.

If you think there are crypto-asset services that should also be added to the EU AML/CFT legal framework obligations, describe the possible risks to tackle:

There are multiple crypto assets circulating already. The holders thereof have not been / will not necessarily be identified in accordance with AMLD V. Not just for AML/CFT reasons such identification may be relevant, but also for market integrity reasons. If for example a pump and dump scheme is performed by one person having multiple wallets, this may not come on the radar. However, if the holder of all these wallets is identified, these multiple transactions may be led back to such individual and the pump and dump scheme could be recognized.

Question 43. If a bespoke framework on crypto-assets is needed, do you consider that all crypto-asset service providers covered by this potential framework should become 'obliged entities' under the EU AML/CFT framework?

Yes. Except in the event that crypto assets are only used for back end solutions. These should be excluded as it will not entail any market integrity risks etc.

Question 44. In your view, how should the AML/CFT risks arising from peer-to-peer transactions (i.e. transactions without intermediation of a service provider) be mitigated?

This is indeed very difficult, comparable to mitigate AML/CFT risks arising from P2P cash payments. One could think of comparable 'maximum' transaction values which can be traded P2P without a CDD obligation to apply or perhaps a reporting obligation to become applicable, but it is questionable to what extent any such rules could be supervised and enforced, in particular if these rules apply to individual, natural persons who may not be aware of any such obligations.

In order to tackle the dangers linked to anonymity, new FATF standards require that "*countries should ensure that originating Virtual Assets Service Providers (VASP) obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should also ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities*" (FATF Recommendations).

Question 45. Do you consider that these requirements should be introduced in the EU AML/CFT legal framework with additional details on their practical implementation?

No, we do not consider these requirements should be introduced in the EU AML/CFT legal framework. In our view step 1 is to subject crypto asset providers to KYC/CDD requirements in order to ensure that any transaction in any crypto asset eventually can be linked to a particular person (natural or legal person). The requirement to submit/share such information is a bridge too far; the requirements should not be heavier/more burdensome that those to which other obliged entities subject to AMLD V are subjected.

Question 46. In your view, do you consider relevant that the following requirements are imposed as conditions for the registration and licensing of providers of services related to crypto-assets included in section III. B?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Directors and senior management of such providers should be subject to fit and proper test from a money laundering point of view, meaning that they should not have any convictions or suspicions on money laundering and related offences	○	○	○	○	◉	○
Service providers must be able to demonstrate their ability to have all the controls in place in order to be able to comply with their obligations under the anti-money laundering framework	○	○	○	○	○	◉

Reasoning: Not all obliged entities under AMLD V (as implemented in the Dutch AML Act are subject to the requirement to 'demonstrate their ability to have all the controls in place in order to be able to comply with their obligations under the anti-money laundering framework' prior to these obliged entities being able to offer their services. As far as a crypto asset service provider is subject to a regulatory license or authorisation obligation, this will be part of its licensing process. However, in our view the rules applicable to crypto asset service providers should not be heavier than for other obliged entities under AMLD V.

3. Consumer/investor protection[21]

Information on the profile of crypto-asset investors and users is limited. Some estimates suggest however that the user base has expanded from the original tech-savvy community to a broader audience, including both retail and institutional investors[22]. Offerings of utility tokens, for instance, do not provide for minimum investment amounts nor are they necessarily limited to professional or sophisticated investors. When considering the consumer protection, the functions of the crypto-assets should also be taken into consideration. While some crypto-assets are bought for investment purposes, other are used as a means of payment or for accessing a specific product or service. Beyond the information that is usually provided by crypto-asset issuer or sponsors in their 'white papers', the question arises whether providers of services related to crypto-assets should carry out suitability checks depending on the riskiness of a crypto-asset (e.g. volatility, conversion risks, ...) relative to a consumer's risk appetite. Other approaches to protect consumers and investors could also include, among others, limits on maximum investable amounts by EU consumers or warnings on the risks posed by crypto-assets.

[21] The term 'consumer' or 'investor' are both used in this section, as the same type of crypto-assets can be bought for different purposes. For instance, payment tokens can be acquired to make payment transactions while they can also be held for investment, given their volatility. Likewise, utility tokens can be bought either for investment or for accessing a specific product or service.

[22] ESMA, "Advice on initial coin offerings and Crypto-Assets", January 2019.

Question 47. What type of consumer protection measures could be taken as regards crypto-assets?

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Information provided by the issuer of crypto-assets (the so-called 'white papers')	○	○	○	○	◉	○
Limits on the investable amounts in crypto-assets by EU consumers	○	○	◉	○	○	○
Suitability checks by the crypto-asset service providers (including exchanges, wallet providers, ...)	○	○	○	◉	○	○
Warnings on the risks by the crypto-asset service providers (including exchanges, platforms, custodial wallet providers, ...)	○	○	○	○	◉	○

Reasoning: The main and first step is ensuring that crypto assets can only be issued upon the issuer having provided a complete, accurate and not-misleading information document/white paper, including the relevant warnings which are already market practice for other types of financial instruments. Although we do not favour yet another form of 'key investor / information document', guidelines or a standardized format for white papers

and crypto assets is not a superfluous luxury. Under the Dutch crowdlending rules, investment limits do apply to retail investors. Although we do not favour such investment limits as in our in view it is an investor's own responsibility to make such judgment, we agree that some Retail investors must be protected against themselves and to safeguard that investors do not loose funds that they need for basic living expenses etc.

47.1 Is there any other type of consumer protection measures that could be taken as regards crypto assets? Please specify which one(s) and explain your reasoning:

Ensure that (retail) investors can only invest with free investable funds, have an offensive investment profile and are fully aware of the risks involved, including in particular not receiving any return on investment and losing their investments in full. Retail investors who do not understand these risks or the difference between crypto assets and other financial products, should be warned not to invest before having obtained advice etc. Issuers and crypto asset service providers could perhaps be subjected to product governance rules comparable to those applicable to manufacturers and distributors under MiFID II.

Question 48. Should different standards of consumer/investor protection be applied to the various categories of crypto-assets depending on their prevalent economic (i.e. payment tokens, stablecoins, utility tokens, ...) or social function?

The consumer/investor protection should, in our view, go hand in hand with the regulatory framework. Due to the multiple appearances of crypto assets, and the continuous development thereof, we doubt whether a distinction should be made between all those different appearances. Rather introduce a framework applicable to crypto assets in the broadest sense and include a clear scope provision as well as, possibly, some exceptions or exemptions to (parts of) the regulatory framework, than to follow different approaches for each particular appearance / type of crypto asset.

Before an actual ICO (i.e. a public sale of crypto-assets by means of mass distribution), some issuers may choose to undertake private offering of crypto-assets, usually with a discounted price (the so-called "private sale"), to a small number of identified parties, in most cases qualified or institutional investors (such as venture capital funds). Furthermore, some crypto-asset issuers or promoters distribute a limited number of crypto-assets free of charge or at a lower price to external contributors who are involved in the IT development of the project (the so-called "bounty") or who raise awareness of it among the general public (the so-called "air drop") (see Autorité des Marchés Financiers, French ICOs – A New Method of financing, November 2018).

Question 49. Should different standards in terms of consumer/investor protection be applied depending on whether the crypto-assets are bought in a public sale or in a private sale?

Reasoning: Yes, we believe that different standards in terms of consumer/investor protection should be applied depending on whether the crypto-assets are bought in a public or private sale. The Prospectus Regulation could in this case be a good example; one on one private sales do not fall under the scope of the PR, whilst public sales (to 150 persons or more) do except if another exception applies like a public offering to qualified investors only. From a Dutch law perspective, at all times an issuer/offeror needs to provide the investor sufficient information to make an informed investment decision. If this obligation does not arise under the PR, it will under Dutch civil laws. We can imagine that a similar path is followed for crypto assets.

Question 50. Should different standards in terms of consumer/investor protection be applied depending on whether the crypto-assets are obtained against payment or for free (e.g. air drops)?

Reasoning: Yes, different standards in terms of consumer/investor protection should be applied depending on whether the crypto-assets are obtained against payment of for free. Currently, offers of securities for free fall out scope of the Prospectus Regulation as well. We do not see a reason why offers of crypto assets for free would require more or better protection than securities.

The vast majority of crypto-assets that are accessible to EU consumers and investors are currently issued outside the EU (in 2018, for instance, only 10% of the crypto-assets were issued in the EU (mainly, UK, Estonia and Lithuania) – Source Satis Research). If an EU framework on the issuance and services related to crypto-assets is needed, the question arises on how those crypto-assets issued outside the EU should be treated in regulatory terms.

Question 51. In your opinion, how should the crypto-assets issued in third countries and that would not comply with EU requirements be treated?

	1 (factor not relevant at all)	2	3	4	5 (very relevant factor)	Don't know / no opinion / not relevant
Those crypto-assets should be banned	○	◉	○	○	○	○
Those crypto-assets should be still accessible to EU consumers/investors	○	○	○	◉	○	○
Those crypto-assets should be still accessible to EU consumers/investors but accompanied by a warning that they do not necessarily comply with EU rules	○	○	○	○	◉	○

Reasoning: Rather a more global (e.g. at G20 level) regulatory approach or guidance is aimed at, simultaneously with investigating an EU framework based on the same principles as currently applicable in respect of other financial instruments.

51.1 Is there any other way the crypto-assets issued in third countries and that would not comply with EU requirements should be treated? Please specify which one(s) and explain your reasoning:

Any offering of crypto assets in the EU irrespective of the jurisdiction of the issuer (in case of an established company issuing such crypto assets; we are not in favour of DAOs) could be subjected to the sane EU rules, similar to the current regulatory framework applicable to securities. We do not see a reason to deviate from that point of departure, albeit that we understand that supervising and enforcement of such rules may be rather difficult.

4. Supervision and oversight of crypto-assets service providers

As a preliminary remark, it should be noted that where a crypto-asset arrangement, including "stablecoin" arrangements qualify as payment systems and/or scheme, the Eurosystem oversight frameworks may apply. In accordance with its mandate, the Eurosystem is looking to apply its oversight framework to innovative projects. As the payment landscape continues to evolve, the Eurosystem oversight frameworks for payments instruments, schemes and arrangements are currently reviewed with a view to closing any gaps that innovative solutions might create by applying a holistic, agile and functional approach. The European Central Bank and Eurosystem will do so in cooperation with other relevant European authorities. Furthermore, the Eurosystem supports the creation of cooperative oversight frameworks whenever a payment arrangement is relevant to multiple jurisdictions. That being said, if a legislation on crypto-assets service providers at EU level is needed, a question arises on which supervisory authorities in the EU should ensure compliance with that regulation, including the licensing of those entities. As the size of the crypto-asset market is still small and does not at this juncture raise financial stability issues, the supervision of the service providers (that are still a nascent industry) by national competent authorities would be justified. At the same time, as some new initiatives (such as the "global stablecoin") through their global reach and can raise financial stability concerns at EU level, and as crypto-assets will be accessible through the internet to all consumers, investors and firms across the EU, it could be sensible to ensure an equally EU-wide supervisory perspective. This could be achieved, inter alia, by empowering the European Authorities (e.g. in cooperation with the European System of Central Banks) to supervise and oversee crypto-asset service providers. In any case, as the crypto-asset market rely on new technologies, EU regulators could face new challenges and require new supervisory and monitoring tools.

Question 52. Which, if any, crypto-asset service providers included in Section III. B do you think should be subject to supervisory coordination or supervision by the European Authorities (in cooperation with the ESCB where relevant) Please explain your reasoning:

With reference to our prior answers, we favour another licensing/authorisation approach than currently applied. We would be in favour of introducing a basic license/authorisation requirement, to be obtained with the relevant NCA, as well as a registration obligation for those undertakings that rely on an exemption, resulting in all crypto asset service providers falling within the scope of the regulatory framework to be known to the NCAs. The basic license/authorisation requirement should ensure compliance with the bare minimum set of obligations relevant to the type of service that the undertaking provides. AML/CFT/KYC/CDD obligations, information obligations, segregation of funds, cybersecurity and integrity of operations and its policymakers are relevant in our view. On the basis of volume indicators or other growth indicators, e.g. on an annual basis, it should be determined whether the undertaking needs to 'step up its license'. The more risks the undertaking brings to the overall financial markets in terms of integrity risk, stability risk, counterparty risk etc. the heavier the license obligations should be. In our view only those undertaking potentially causing stability risks to the EU financial markets as a whole should be supervised by the relevant ESAs. Provided there will be clear guidance and an harmonised regulatory framework throughout the EEA, we do not see a reason why NCAs cannot supervise the undertakings / crypto asset service providers falling under their home member state control.

Question 53. Which are the tools that EU regulators would need to adequately supervise the crypto-asset service providers and their underlying technologies?

- Deep knowledge and understanding of all the technological aspects relevant to crypto assets, such as DLT itself, the different types of blockchains used, consensus protocols used, algorithms, programming, smart contracts, APIs, AI, use of oracles and other technological input used by algorithms underlying the crypto assets, etc;
- Access to all data on the relevant blockchains used for (transaction reporting), monitoring and enforcement purposes;
- Algorithms that can be run against those data to signal peculiarities;
- ESAs (not NCAs) should have authority to stop the trading of a particular crypto asset to be used in very rare circumstances only.

IV. Crypto-assets that are currently covered by EU legislation

This last part of the public consultation consists of general questions on security tokens (A.), an assessment of legislation applying to security tokens (B.) and an assessment of legislation applying to e-money tokens (C.).

A. General questions on 'security tokens'

Introduction

For the purpose of this section, we use the term 'security tokens' to refer to crypto-assets issued on a DLT and that qualify as transferable securities or other types of MiFID financial instruments. By extension, activities concerning security tokens would qualify as MiFID investment services/activities and transactions in security tokens admitted to trading or traded on a trading venue[23] would be captured by MiFID provisions. Consequently, firms providing services concerning security tokens should ensure they have the relevant MiFID authorisations and that they follow the relevant rules and requirements. MiFID is a cornerstone of the EU regulatory framework as financial instruments covered by MiFID are also subject to other financial legislation such as CSDR or EMIR, which therefore equally apply to post-trade activities related to security tokens.

Building on ESMA's advice on crypto-assets and ICOs issued in January 2019 and on a preliminary legal assessment carried out by Commission services on the applicability and suitability of the existing EU legislation (mainly at level 1[24]) on trading, post-trading and other financial services concerning security tokens, such as asset management, the purpose of this part of the consultation is to seek stakeholders' views on the issues identified below that are relevant for the application of the existing regulatory framework to security tokens.

Technology neutrality is one of the guiding principles of the Commission's policies. A technologically neutral approach means that legislation should not mandate market participants to use a particular type of technology. It is therefore crucial to address any obstacles or identify any gaps in existing EU laws which could prevent the take-up of financial innovation, such as DLT, or leave certain risks brought by these innovations unaddressed. In parallel, it is also important to assess whether the market practice or rules at national level could facilitate or be an impediment that should also be addressed to ensure a consistent approach at EU level.

[23] Trading venues are a regulated market, a multilateral trading facility or an organised trading facility.

[24] At level 1, the European Parliament and Council adopt the basic laws proposed by the Commission, in the traditional co- decision procedure. At level 2 the Commission can adopt, adapt and update technical implementing measures with the help of consultative bodies composed mainly of EU countries representatives. Where the level 2 measures require the expertise of supervisory experts, it can be determined in the basic act that these measures are delegated or implemented acts based on draft technical standards developed by the European supervisory authorities.

Current trends concerning security tokens

For the purpose of the consultation, we consider the instances where security tokens would be admitted to trading or traded on a trading venue within the meaning of MiFID. So far, however, there is evidence of only a few instances of security tokens issuance[25], with none of them having been admitted to trading or traded on a trading venue nor admitted in a CSD book-entry system[26].

Based on the limited evidence available at supervisory and regulatory level, it appears that existing requirements in the trading and post-trade area would largely be able to accommodate activities related to security tokens via permissioned networks and centralised platforms[27]. Such activities would be overseen by a central body or operator, de facto similarly to traditional market infrastructures such as multilateral trading venues or central security depositories. Based on the limited evidence currently available from the industry, it seems that activities related to security tokens would most likely develop via authorised centralised solutions. This could be driven by the relative efficiency gain that the use of the legacy technology of a central provider can generally guarantee (with near-instantaneous speed and high liquidity with large volumes), along with the business expertise of the central provider that would also ensure higher investor protection and easier supervision and enforcement of the rules.

On the other hand, it seems that adjustment of existing EU rules would be required to allow for the development of permissionless networks and decentralised platforms where activities would not be entrusted to a central body or operator but would rather occur on a peer-to-peer[28] basis. Given the absence of a central body that would be accountable for enforcing the rules of a public market, trading and post-trading on permissionless networks could also potentially create risks as regards market integrity and financial stability, which are regarded as being of utmost importance by the EU financial acquis.

The Commission services' understanding is that permissionless networks and decentralised platforms[29] are still in their infancy, with uncertain prospects for future applications in financial services due to their higher trade latency and lower liquidity. Permissionless decentralised platforms could potentially develop only at a longer time horizon when further maturing of the technology would provide solutions for a more efficient trading architecture. Therefore, it could be premature at this point in time to make any structural changes to the EU regulatory framework.

Security tokens are, in principle, covered by the EU legal framework on asset management in so far as such security tokens fall within the scope of "financial instrument" under MiFID II. To date, however, the examples of the regulatory use cases of DLT in the asset management domain have been incidental.

To conclude, depending on the feedback to this consultation, a gradual regulatory approach might be considered, trying to provide first legal clarity to market participants as regards permissioned networks and centralised platforms before considering changes in the regulatory framework to accommodate permissionless networks and decentralised platforms.

At the same time, the Commission services would like to use this opportunity to gather views on market trends as regards permissionless networks and decentralised platforms, including their potential impact on current business models and the possible regulatory approaches that may be needed to be considered, as part of a second step. A list of questions is included after the assessment by legislation.

[25] For example the German Fundament STO which received the authorisation from Bafin in July 2019

[26] See section IV.2.5 for further information

[27] Type of crypto-asset trading platforms 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.

[28] In the trading context, going peer-to-peer means having participants buy and sell assets directly with each other, rather than working through an intermediary or third party service

[29] Type of crypto-asset trading platforms that do not hold crypto-assets on behalf of its clients. The trade settlement usually takes place on the DLT itself, i.e. on-chain.

Question 54. Please highlight any recent market developments (such as issuance of security tokens, development or registration of trading venues for security tokens, ...) as regards security tokens (at EU or national level)?

The trend that we see in our daily practice is that the interest in STOs is decreasing and that initiatives in respect of trading venues for security tokens are being considered but held off for now due to the heavy MiFID regulatory framework applicable to it and the relative infant stage of the market.

Question 55. Do you think that DLT could be used to introduce efficiencies or other benefits in the trading, post-trade or asset management areas?

Completely agree. Reasoning: we believe in DLT as the technology that can bring the efficiency and also integrity of the financial markets to the next level, thanks to its characteristics of transparency and immutability. We do note that permissionless networks to that end could have more advantages than permissioned networks, depending on the network protocol. It is important to have a robust network and that it is not one or more colluding nodes can bring detrimental effect to the integrity of the network. However, we can imagine that a centralized platform can be preferred over a decentralized platform, where the operator of the platform, comparable to an operator of a regulated market/MTF/OTF, ensures that trading takes place in accordance with the market (integrity) rules applicable to such 'trading venue'.

If you agree with question 55, please indicate the specific areas where, in your opinion, the technology could afford most efficiencies when compared to the legacy system:

- Settlement of transactions (transparent, immutable, quick)
- Possibly, in case of on chain settlement, no or limited counterparty risk, resulting in less need for clearing
- Automatic transaction reporting on the basis of the data that can be extracted automatically from the relevant blockchain and sent or directly reviewed by the NCAs;
- MAR analysis possibly easier?
- P2P on chain trading would result in lower transaction costs, but - if there are no market makers or alike investors who can indicate bid ask spreads etc., P2P trading may also have a negative impact on market integrity and pricing of the crypto assets involved. It should be considered whether MAR should be applicable to trading activities in respect of crypto assets, but we also find it important that trading is stimulated without a network or platform offering a 'trading venue' immediately being required to obtain a MiFID II license for operating an MTF (or OTF).

Question 56. Do you think that the use of DLT for the trading and post-trading of financial instruments poses more financial stability risks when compared to the traditional trading and post-trade architecture?

Rather disagree. Reasoning: in our view the characteristics of DLT may result in less financial stability risks due to the inherent transparency. However, trading on a blockchain does require rules comparable to the ones currently applicable to traditional trading venues.

Question 57. Do you consider that DLT will significantly impact the role and operation of trading venues and post-trade financial market infrastructures (CCPs, CSDs) in the future (5/10 years' time)? Please explain your reasoning.

Yes; please see our prior response. Clearing, and therefore CCPs, may become of less relevance in case of P2P on chain trading via DLT. Settlement will take place instantly as well, so the same may apply to CSDs. However, in centralised platforms where trading takes place via the operator of the platform, the operator will presumably take a position comparable to systematic internalisers under MiFID II, either by executing client orders against their own books or against other clients/users of the platform.

Question 58. Do you agree that a gradual regulatory approach in the areas of trading, post-trading and asset management concerning security tokens (e.g. provide regulatory guidance or legal clarification first regarding permissioned centralised solutions) would be appropriate?

Rather disagree. Reasoning: presumably trading, post trading and asset management concerning security tokens simply fall under the scope of MiFID II and therefore under an existing regulatory framework already. It is questionable whether these platforms/offerors of such solutions should be subjected to a full MiFID II regime, and in particular the one applicable to operators of trading venues within the meaning of MiFID II/MiFIR. Despite the point of departure of tech neutrality, which we agree to, we are in favour of the introduction of a light MiFID regime (comparable to the one introduced in the draft Crowdfunding Regulation, though with special rules in respect of trading of the tokens) or a 'basic license requirement' which grows with the operator / undertaking offering these type of crypto asset (trading) services with license (and corresponding obligations) grow with the undertaking on the basis of certain volume indicators. A more proportionate regime which is both available to small existing investment firms as well as undertakings that contemplate to offer this type of crypto asset services. In addition to that special attention needs to be paid to AML/CFT rules as well as MAR.

B. Assessment of legislation applying to 'security tokens'

1. Market in Financial Instruments Directive framework (MiFID II)

The Market in Financial Instruments Directive framework consists of a directive (MiFID) and a regulation (MiFIR) and their delegated acts. MiFID II is a cornerstone of the EU's regulation of financial markets seeking to improve their competitiveness by creating a single market for investment services and activities and to ensure a high degree of harmonised protection for investors in financial instruments. In a nutshell MiFID II sets out: (i) conduct of business and organisational requirements for investment firms; (ii) authorisation requirements for regulated markets, multilateral trading facilities, organised trading facilities and broker/dealers; (iii) regulatory reporting to avoid market abuse; (iv) trade transparency obligations for equity and non-equity financial instruments; and (v) rules on the admission of

financial instruments to trading. MiFID also contains the harmonised EU rulebook on investor protection, retail distribution and investment advice.

1.1 Financial instruments

Under MiFID, financial instruments are 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. Under Article 4(1)(15), 'transferable securities' notably means those classes of securities which are negotiable on the capital market, with the exception of instruments of payment.

There is currently no legal definition of security tokens in the EU financial services legislation. Indeed, in line with a functional and technologically neutral approach to different categories of financial instruments in MiFID, where security tokens meet necessary conditions to qualify as a specific type of financial instruments, they should be regulated as such. However, the actual classification of a security token as a financial instrument is undertaken by National Competent Authorities (NCAs) on a case-by-case basis.

In its Advice, ESMA indicated that in transposing MiFID into their national laws, the Member States have defined specific categories of financial instruments differently (i.e. some employ a restrictive list to define transferable securities, others use broader interpretations). As a result, while assessing the legal classification of a security token on a case by case basis, Member States might reach diverging conclusions. This might create further challenges to adopting a common regulatory and supervisory approach to security tokens in the EU.

Furthermore, some 'hybrid' crypto-assets can have 'investment-type' features combined with 'payment-type' or 'utility-type' characteristics. In such cases, the question is whether the qualification of 'financial instruments' must prevail or a different notion should be considered.

Question 59. Do you think that the absence of a common approach on when a security token constitutes a financial instrument is an impediment to the effective development of security tokens?

Completely agree. Reasoning: it is of the essence, in line with the Single Market rules, that defined terms in Level 1 EU legislation are interpreted in the same manner. Our answer goes beyond crypto assets / security tokens. In the Netherlands, the general approach is that any negotiable (a) equity or equity-like, (b) debt or debt-like, and

(c) options to obtain any instruments as meant under (a) or (b) are considered securities within the meaning of MiFID II. A financial instrument is considered to be negotiable if it is (i) freely transferable, (ii) standardized

/interchangeable and (iii) could by its nature trade on financial markets (whilst it does not need to be admitted to trading on any trading venue). Generally, any share in a Dutch company is considered negotiable. Debt instruments give you a bit more leeway, as the terms can explicitly exclude transferability of the debt instruments, resulting in those not qualifying as securities within the meaning of MiFID II as implemented in Dutch law. Similar qualification issues arise in respect of security tokens, but in our view any crypto asset that

can actually be transferred, will easily meet the Dutch interpretation of security within the meaning of MiFID II. This results in the Dutch interpretation that security tokens generally are securities within the meaning of MiFID II and resulting the issuer to be subjected to the Prospectus Regulation and any intermediary (including wallet providers) to potentially be subject to MiFID II license requirements as broker, asset manager or possibly an operator of a trading venue such as an MTF or OTF. To prevent regulatory arbitrage and to limit complexity and market integrity risks as much as possible, it is important that there will be a harmonised EU approach to any type of crypto assets, including security tokens. Currently issuers of security tokens (as well as investors) are treated differently within the EEA in respect of the same whitepaper and the same security token. This is an impediment to the proper functioning of the Single Market.

Question 60. If you consider that the absence of a common approach on when a security token constitutes a financial instrument is an impediment, what would be the best remedies according to you?

	1 (factor not relevant at all)	2	3	4	5 (very relevant factor)	Don't know / no opinion / not relevant
Harmonise the definition of certain types of financial instruments in the EU	○	○	○	○	◉	○
Provide a definition of a security token at EU level	○	○	○	○	◉	○
Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token	○	○	○	◉	○	○

Reasoning: We defer to our response to question 59. As to the statement as to the importance to 'provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token', it should be taken into account that chances are that this could complicate things as well because it could lead to even more hybrid/alternative appearances of crypto assets in respect of which NCAs as well as professional advisors may have trouble qualifying these and determining the applicable regulatory framework if the token have some but not all listed criteria etc. That would again result in a non- harmonised approach within the EEA.

Question 61. How should financial regulators deal with hybrid cases where tokens display investment-type features combined with other features (utility-type or payment-type characteristics)?

	1 (factor not relevant at all)	2	3	4	5 (very relevant factor)	Don't know / no opinion / not relevant
Hybrid tokens should qualify as financial instruments/security tokens	○	○	○	○	◉	○
Hybrid tokens should qualify as unregulated crypto-assets (i.e. like those considered in section III. of the public consultation document)	○	◉	○	○	○	○
The assessment should be done on a case-by-case basis (with guidance at EU level)	◉	○	○	○	○	○

61.1 Is there any other way financial regulators should deal with hybrid cases where tokens display investment-type features combined with other features?

As mentioned before, it should be clear from the outset which regulatory framework applies to crypto assets, including hybrid crypto assets. Clarity in this respect is important for all stakeholders. It serves legal certainty. We have seen in the crypto markets that features of a crypto asset can change overtime without the issuer having any role in that respect. If an unregulated form of crypto asset develops into a more investment-type crypto asset, it should not all of the sudden become subject to another regulatory framework. In our view, only very limited appearances of crypto assets could remain unregulated.

1.2. Investment firms

According to Article 4(1)(1) and Article 5 of MiFID, all legal persons offering investment services/activities in relation to financial instruments need be authorised as investment firms to perform those activities/services. The actual authorisation of an investment firm is undertaken by the NCAs with respect to the conditions, requirements and procedures to grant the authorisation. However, the application of these rules to security tokens may create challenges, as they were not designed with these instruments in mind.

Question 62. Do you agree that existing rules and requirements for investment firms can be applied in a DLT environment?

Rather agree. Reasoning: these rules can form the basis, but could be not proportionate to the size of the company / risks involved. We defer to our other answers in which we have explained our preference for a 'basic licensing/authorisation requirement' or 'MiFID light regime comparable to the regime introduced in the (draft) Crowdfunding Regulation.

Question 63. Do you think that a clarification or a guidance on applicability of such rules and requirements would be appropriate for the market?

Completely agree. Reasoning: we defer to our answer provided to question 6.

1.3 Investment services and activities

Under MiFID Article 4(1)(2), investment services and activities are specified in Section A of Annex I, such as 'reception and transmission of orders, execution of orders, portfolio management, investment advice, etc. A number of activities related to security tokens are likely to qualify as investment services and activities. The organisational requirements, the conduct of business rules and the transparency and reporting requirements laid down in MiFID II would also apply, depending on the types of services offered and the types of financial instruments.

Question 64. Do you think that the current scope of investment services and activities under MiFID II is appropriate for security tokens?

Rather agree. Reasoning: not just security tokens; any crypto assets that qualify as financial instruments (such as derivatives with crypto assets as an underlying value). In terms of proportionality of the regime, we kindly defer you to our answer to questions 14 and 15 relating to our suggestion to introduce a basic authorisation requirement.

Question 65. Do you consider that the transposition of MiFID II into national laws or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT for investment services and activities? Please explain your reasoning.

Almost all our clients who contemplated to offer services in respect of crypto assets that qualify as financial instruments within the meaning of MiFID II (such as security tokens) have decided to await a further development of the crypto market before expanding their services to such types of crypto assets after they were informed of the MiFID II implications to their plans. The framework applicable to investment firms is difficult; not just because of the incredible amount of detailed rules but also because not all of them are easily applied in respect of crypto assets. Obtaining a MiFID II license is a long and costly exercise, but even more so for crypto asset service providers who need to substantiate to the NCA any deviation from a specific MiFID II rule/obligation which deviation is caused by the nature of crypto assets.

Whilst there is an initiative for a regulatory sandbox in the Netherlands, none of these types of projects/ crypto asset service providers are admitted (to our knowledge). The main reason is that the Dutch NCAs are limited in offering other forms of authorisation if they hold the view that a license obligation applies on the basis of the existing EU framework, such as MiFID II. We would favour either a sandbox on EU level or guidance provided by the ESAs to the NCAs in respect of the terms and conditions that could apply to local sandboxes irrespective of the existing EU regulatory framework. This would, in our view, stimulate innovation ánd knowledge sharing between the relevant stakeholders.

1.4. Trading venues

Under MiFID Article 4(1)(24) 'trading venue' means a regulated market (RM), a Multilateral Trading Facility (MTF) or an Organised Trading Facility (OTF') which are defined as a multilateral system operated by a market operator or an investment firm, bringing together multiple third-party buying and selling interests in financial instruments. This means that the market operator or an investment firm must be an authorised entity, which has legal personality.

As also reported by ESMA in its advice, platforms which would engage in trading of security tokens may fall under three main broad categories as follows:

- *Platforms with a central order book and/or matching orders would qualify as multilateral systems;*
- *Operators of platforms dealing on own account and executing client orders against their proprietary capital, would not qualify as multilateral trading venues but rather as investment firms; and*
- *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 (recital 8 of MiFIR).*

Question 66. Would you see any particular issues (legal, operational) in applying trading venue definitions and requirements related to the operation and authorisation of such venues to a DLT environment which should be addressed? Please explain your reasoning.

Not necessarily, but we highly favour more guidance on the difference between bulletin boards and MiFID trading venues (in particular MTFs/OTFs). We favour on chain trading because of its transparency of the transactions being captured in the 'register'/blockchain, but we expect that this would raise qualification questions in respect of the operator of the platform offering such trading opportunities. The Dutch Authority for the Financial Markets (as well as the Dutch government) is not a supporter of bulletin boards. We expect the Dutch NCA to qualify any platform on which the trade is settled on chain to be a trading venue within the meaning of MiFID II. The regulatory implications for such operator are huge. And at the same time, many of those regulatory obligations may be superfluous if the NCAs have access to the data on the relevant blockchain on which the trades are settled. Transaction reporting obligations for example may no longer be needed if this is done automatically.

1.5. Investor protection

A fundamental principle of MiFID II (Articles 24 and 25) is to ensure that investment firms act in the best interests of their clients. Firms shall prevent conflicts of interest, act honestly, fairly and professionally and execute orders on terms most favourable to the clients. With regard to investment advice and portfolio management, various information and product governance requirements apply to ensure that the client is provided with a suitable product.

Question 67. Do you think that current scope of investor protection rules (such as information documents and the suitability assessment) are appropriate for security tokens? Please explain your reasoning.

The technology and legal peculiarities behind the investment asset itself, does not really matter in our view. As an example: many securities are nowadays in registered form; the investor only sees them registered in its investment account that the investor holds with its investment firm/broker/custodian/bank. In the back end administrations, many of these registered shares are issued in book-entry form, resulting in for example the CSD being the legal owner of the shares and the investors only having a share in the girodepot of a CSD. This is not common knowledge of all investors, and it does not really matter either. There are technical and legal means to ensure that the investor's assets are segregated from the assets of its investment firm/broker/custodian/bank.

The legal qualification and forthcoming of a crypto asset as a security token will, presumably, not be known or understood by (retail) investors. Also the exact technology behind the crypto asset will, presumably, be unknown territory for many (Retail) investors. But similar to registered shares offered in book-entry form, investors do not necessarily need to be informed in respect of all such technical details. Their main interest is to be accurately and adequately informed of their rights (and obligations) and the risks involved when they decide to invest their funds in any crypto asset, including security tokens. In our view, at a bare minimum it should be safeguarded that any investor is being provided with the information needed for it to make an informed investment decision in respect of a particular crypto asset. Retail investors may need to be protected against themselves and be subjected to a suitability assessment.

Question 68. Would you see any merit in establishing specific requirements on the marketing of security tokens via social media or online? Please explain your reasoning.

No other marketing rules than already existing and applicable at this stage.

Question 69. Would you see any particular issue (legal, operational,) in applying MiFID investor protection requirements to security tokens? Please explain your reasoning.

Not at this stage.

1.6. SME growth markets

To be registered as SME growth markets, MTFs need to comply with requirements under Article 33 (e.g. 50% of SME issuers, appropriate criteria for initial and ongoing admission, effective systems and controls to prevent and detect market abuse). SME growth markets focus on trading securities of SME issuers. The average number of transactions in SME securities is significantly lower than those with large capitalisation and therefore less dependent on low latency and high

throughput. Since trading solutions on DLT often do not allow processing the amount of transactions typical for most liquid markets, the Commission is interested in gathering feedback on whether trading on DLT networks could offer cost efficiencies (e.g. lower costs of listing, lower transaction fees) or other benefits for SME Growth Markets that are not necessarily dependent on low latency and high throughput.

Question 70. Do you think that trading on DLT networks could offer cost efficiencies or other benefits for SME Growth Markets that do not require low latency and high throughput? Please explain your reasoning.

Yes, we defer to our answers to questions 37.2 and 38.

1.7. Systems resilience, circuit breakers and electronic trading

According to Article 48 of MiFID, Member States shall require a regulated market to have in place effective systems, procedures and arrangements to ensure its trading systems are resilient, have sufficient capacity and fully tested to ensure orderly trading and effective business continuity arrangements in case of system failure. Furthermore regulated markets that permits direct electronic access[30] shall have in place effective systems procedures and arrangements to ensure that members are only permitted to provide such services if they are investment firms authorised under MiFID II or credit institutions. The same requirements also apply to MTFs and OTFs according to Article 18(5). These requirements could be an issue for security tokens, considering that crypto-asset trading platforms typically provide direct access to retail investors.

[30] As defined by article 4(1)(41) and in accordance with Art 48(7) of MIFID by which trading venues should only grant permission to members or participants to provide direct electronic access if they are investment firms authorised under MiFID or credit institutions authorised under the Credit Requirements Directive (2013/36/EU)

Question 71. Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed? Please explain your reasoning.

No opinion at this stage.

1.8. Admission of financial instruments to trading

In accordance with Article 51 of MiFID, regulated markets must establish clear and transparent rules regarding the admission of financial instruments to trading as well as the conditions for suspension and removal. Those rules shall ensure that financial instruments admitted to trading on a regulated market are capable of being traded in a fair, orderly and efficient manner. Similar requirements apply to MTFs and OTFs according to Article 32. In short, MiFID lays down general principles that should be embedded in the venue's rules on admission to trading, whereas the specific rules are established by the venue itself. Since markets in security tokens are very much a developing phenomenon, there may be merit in reinforcing the legislative rules on admission to trading criteria for these assets.

Question 72. Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed? Please explain your reasoning.

TBD whether a blockchain based order routing system qualifies as algorithmic trading, in particular in respect of a blockchain with smart contract functionality (assuming the smart contract indeed 'acts' on pre- determined parameters/triggers and results in one or more individual parameters of an order to be automatically determined by the smart contract).

Question 1.9 Access to a trading venues

In accordance with Article 53(3) and 19(2) of MiFID, RMs and MTFs may admit as members or participants only investment firms, credit institutions and other persons who are of sufficient good repute; (b) have a sufficient level of trading ability, competence and ability (c) have adequate organisational arrangements; (d) have sufficient resources for their role. In effect, this excludes retail clients from gaining direct access to trading venues. The reason for limiting this kind of participants in trading venues is to protect investors and ensure the proper functioning of the financial markets. However, these requirements might not be appropriate for the trading of security tokens as crypto-asset trading platforms allow clients, including retail investors, to have direct access without any intermediation.

Question 73. What are the risks and benefits of allowing direct access to trading venues to a broader base of clients? Please explain your reasoning.

Benefits would naturally be the cost efficiencies for the (retail) investor due to middlemen being cut out of the chain. On chain settlement is also beneficial, as it limits counterparty risks to a great extent. However, if any (retail) investor has direct access to crypto asset trading venues, this may trigger market integrity risks as sophisticated investors may take advantage of (Retail) investors' incompetence. We do not see a reason why other access rules should be available to investors in respect of crypto asset trading venues compared to trading venues on which financial instruments within the meaning of MiFID II are traded. We therefore doubt whether (Retail) investors should be allowed direct access to trading venues in respect of trading crypto assets.

1.10 Pre and post-transparency requirements

In its Articles 3 to 11, MiFIR sets out transparency requirements for trading venues in relations to both equity and non-equity instruments. In a nutshell for equity instruments, it establishes pre-trade transparency requirements with certain waivers subject to restrictions (i.e. double volume cap) as well as post-trade transparency requirements with authorised deferred publication. Similar structure is replicated for non-equity instruments. These provisions would apply to security tokens. The availability of data could perhaps be an issue for best execution[31] ~~of~~ security tokens platforms. For the transparency requirements, it could perhaps be more difficult to establish meaningful transparency thresholds according to the calibration specified in MIFID, which is based on EU wide transaction data. However, under current circumstances, it seems difficult to clearly determine the need for any possible adaptations of existing rules due to the lack of actual trading of security tokens.

[31] MiFID II investment firms must take adequate measures to obtain the best possible result when executing the client's orders. This obligation is referred to as the best execution obligation.

Question 74. Do you think these pre- and post-transparency requirements are appropriate for security tokens?

Yes, but we note that the actual advantage of (on chain) trading is the transparency already captured by the blockchain. We would favour access rights for the NCAs to the blockchain on which the trading venue runs (assuming on chain trading) in order for the relevant (post) trade transaction data to be extracted/copied from the blockchain.

Question 75. Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed (e.g. in terms of availability of data or computation of thresholds)? Please explain your reasoning.

Not at this stage.

1.11. Transaction reporting and obligations to maintain records

In its Article 25 and 26, MiFIR sets out detailed reporting requirements for investment firms to report transactions to their competent authority. The operator of the trading venue is responsible for reporting the details of the transactions where the participants is not an investment firm. MiFIR also obliges investment firms or the operator of the trading venue to maintain records for five years. Provisions would apply to security tokens very similarly to traditional financial instruments. The availability of all information on financial instruments required for reporting purposes by the Level 2 provisions could perhaps be an issue for security tokens (e.g. ISIN codes are mandatory).

Question 76. Would you see any particular issue (legal, operational) in applying these requirement to security tokens which should be addressed? Please explain your reasoning.

With reference to the above, questionable whether these obligations are needed in case of on chain trading and an automatic data flow to the relevant NCAs (or ESA) to be programmed in the protocol of the blockchain on which the trading venue runs.

2. Market Abuse Regulation (MAR)

MAR establishes a comprehensive legislative framework at EU level aimed at protecting market integrity. It does so by establishing rules around prevention, detection and reporting of market abuse. The types of market abuse prohibited in MAR are insider dealing, unlawful disclosure of inside information and market manipulation. The proper application of the MAR framework is very important for guaranteeing an appropriate level of integrity and investor protection in the context of trading in security tokens.

Security tokens are covered by the MAR framework where they fall within the scope of that regulation, as determined by its Article 2. Broadly speaking, this means that all transactions in security tokens admitted to trading or traded on a trading venue (under MiFID Article 4(1)(24) 'trading venue' means a regulated market (RM), a Multilateral Trading Facility (MTF) or an Organised Trading Facility (OTF')) are captured by its provisions, regardless of whether transactions or orders in those tokens take place on a trading venue or are conducted over-the-counter (OTC).

2.1. Insider dealing

Pursuant to Article 8 of MAR, insider dealing arises where a person possesses inside information and uses that information by acquiring or disposing of, for its own account or for the account of a third party, directly or indirectly, financial instruments to which that information relates. In the context of security tokens, it might be the case that new actors, such as miners or wallet providers, hold new forms of inside information and use it to commit market abuse. In this regard, it should be noted that Article 8(4) of MAR contains a catch-all provision applying the notion of insider dealing to all persons who possess inside information other than in circumstances specified elsewhere in the provision.

Question 77. Do you think that the current scope of Article 8 of MAR on insider dealing is appropriate to cover all cases of insider dealing for security tokens? Please explain your reasoning.

No, not necessarily because of Article 8 MAR, but due to the current fact that:

- currently (to our knowledge) no security token is admitted to a trading venue that falls under the scope of the MAR;
- the scope of MAR is broader than securities; it includes any financial instruments admitted to trading on a trading venue (i.e. a regulated market, MTF or OTF). As such any crypto asset qualifying as a financial instrument and admitted to such a trading venue would fall under the scope of MAR;

To that end we hold the view that trading in crypto assets that fall (now or PM) under a regulatory framework should fall under the scope of the main prohibitions under MAR (such as prohibition on insider dealing, market manipulation, tipping prohibition). At this stage of the crypto market and the volatility on the crypto asset prices, we are of the opinion that the requirement to publish price sensitive information and to have insider lists etc. may be less relevant to (issuers of) crypto assets.

2.2. Market manipulation

In its Article 12(1)(a), MAR defines market manipulation primarily as covering those transactions and orders which (i) give false or misleading signals about the volume or price of financial instruments or (ii) secure the price of a financial instrument at an abnormal or artificial level. Additional instances of market manipulation are described in paragraphs (b) to (d) of Article 12(1) of MAR.

Since security tokens and blockchain technology used for transacting in security tokens differ from how trading of traditional financial instruments on existing trading infrastructure is conducted, it might be possible for novel types of market manipulation to arise that MAR does not currently address. Finally, there could be cases where a certain financial instrument is covered by MAR but a related unregulated crypto-asset is not in scope of the market abuse framework. Where there would be a correlation in values of such two instruments, it would also be conceivable to influence the price or value of one through manipulative trading activity of the other.

Question 78. Do you think that the notion of market manipulation as defined in Article 12 of MAR is sufficiently wide to cover instances of market manipulation of security tokens? Please explain your reasoning.

Yes. As to the statement 'there could be cases where a certain financial instrument is covered by MAR but a related unregulated crypto-asset is not in scope of the market abuse framework. Where there would be a correlation in values of such two instruments, it would also be conceivable to influence the price or value of one through manipulative trading activity of the other.', we agree that this possibility should be prevented. As mentioned before, in our view only very limited appearances of crypto assets should not be regulated, resulting in the majority to be regulated forms of crypto assets. Part of the regulatory framework should, in our view, be applicability of the main prohibitions as laid down in MAR. At that stage, this identified risk of 'derivative market abuse' will be mitigated.

Question 79. Do you think that there is a particular risk that manipulative trading in crypto-assets which are not in the scope of MAR could affect the price or value of financial instruments covered by MAR?

No opinion at this stage.

4. Prospectus Regulation (PR)

The Prospectus Regulation establishes a harmonised set of rules at EU level about the drawing up, structure and oversight of the prospectus, which is a legal document accompanying an offer of securities to the public and/or an admission to trading on a regulated market. The prospectus describes a company's main line of business, its finances, its shareholding structure and the securities that are being offered and/or admitted to trading on a regulated market. It contains the information an investor needs before making a decision whether to invest in the company's securities.

4.1. Scope and exemptions

With the exception of out of scope situations and exemptions (Article 1(2) and (3)), the PR requires the publication of a prospectus before an offer to the public or an admission to trading on a regulated market (situated or operating within a Member State) of transferable securities as defined in MiFID II. The definition of 'offer of securities to the public' laid down in Article 2(d) of the PR is very broad and should encompass offers (e.g. STOs) and advertisement relating to security tokens. If security tokens are offered to the public or admitted to trading on a regulated market, a prospectus would always be required unless one of the exemptions for offers to the public under Article 1(4) or for admission to trading on a RM under Article 1(5) applies.

Question 82. Do you consider that different or additional exemptions should apply to security tokens other than the ones laid down in Article 1(4) and Article 1(5) of PR?

Completely disagree. Reasoning: as already elaborated upon in other answers, in our view the PR gives a clear framework for the obligation to publish a 'Prospectus Regulation proof' prospectus. We do not see any reason why this framework would not apply to crypto assets qualifying as securities such as security tokens. That being said, we do favour a standardized information document providing minimum information to investors ensuring that they can make an informed investment decision. We defer to our answer to question 21 in this respect.

4.2. The drawing up of the prospectus

Delegated Regulation (EU) 2019/980, which lays down the format and content of all the prospectuses and its related documents, does not include schedules for security tokens. However, Recital 24 clarifies that, due to the rapid evolution of securities markets, where securities are not covered by the schedules to that Regulation, national competent authorities should decide in consultation with the issuer which information should be included in the prospectus. Such approach is meant to be a temporary solution. A long term solution would be to either (i) introduce additional and specific schedules for security tokens, or (ii) lay down 'building blocks' to be added as a complement to existing schedules when drawing up a prospectus for security tokens.

The level 2 provisions of prospectus also defines the specific information to be included in a prospectus, including Legal Entity Identifiers (LEIs) and ISIN. It is therefore important that there is no obstacle in obtaining these identifiers for security tokens.

The eligibility for specific types of prospectuses or relating documents (such as the secondary issuance prospectus, the EU Growth prospectus, the base prospectus for non-equity securities or the universal registration document) will depend on the specific types of transferable securities to which security tokens correspond, as well as on the type of the issuer of those securities (i.e. SME, mid-cap company, secondary issuer, frequent issuer).

Article 16 of PR requires issuers to disclose risk factors that are material and specific to the issuer or the security, and corroborated by the content of the prospectus. ESMA's guidelines on risk factors under the PR assist national competent authorities in their review of the materiality and specificity of risk factors and of the presentation of risk factors across categories depending on their nature. The prospectus could include pertinent risks associated with the underlying technology (e.g. risks relating to technology, IT infrastructure, cyber security, etc, ...). ESMA's guidelines on risk factors could be expanded to address the issue of materiality and specificity of risk factors relating to security tokens.

Question 83. Do you agree that Delegated Regulation (EU) 2019/980 should include specific schedules about security tokens?

No, we defer to our answer to question 67 in this respect.

Question 84. Do you identify any issues in obtaining an ISIN for the purpose of issuing a security token?

In our view, any crypto asset that can be traded should have an ISIN, not just security tokens. As long as crypto assets (including security tokens) are recognized by ANNA / ISIN issuing organization (preferably as a separate asset class), we do not see any issues in obtaining an ISIN for such crypto assets. We do not have knowledge of the underlying ISO requirements which may need to be amended for crypto assets.

Question 85. Have you identified any difficulties in applying special types of prospectuses or related documents (i.e. simplified prospectus for secondary issuances, the EU Growth prospectus, the base prospectus for non-equity securities, the universal registration document) to security tokens that would require amending these types of prospectuses or related documents? Please explain your reasoning.

No, not yet.

Question 86. Do you believe that an ad hoc alleviated prospectus type or regime (taking as example the approach used for the EU Growth prospectus or for the simplified regime for secondary issuances) should be introduced for security tokens?

No. The existing simplified regimes and EU growth prospectus rules etc. can be applied to issuers of security tokens if they satisfy the conditions applicable to such regime. The mere fact that an issuer raises money by offering security tokens is not a reason for an alleviated prospectus type or regime in our view.

Question 87. Do you agree that issuers of security tokens should disclose specific risk factors relating to the use of DLT?

DLT should be explained, and particular risks relating to the use of DLT such as, possibly, privacy risks and the risks relating to the immaturity of the crypto asset (trading) market, such as volatility risks, limited liquidity risks, etc. should be addressed, but in general the technology behind it will presumably not be the main interest of most investors.

5. Central Securities Depositories Regulation (CSDR)

CSDR aims to harmonise the timing and conduct of securities settlement in the European Union and the rules for central securities depositories (CSDs) which operate the settlement infrastructure. It is designed to increase the safety and efficiency of the system, particularly for intra-EU transactions. In general terms, the scope of the CSDR refers to the 11 categories of financial instruments listed under MiFID. However, various requirements refer only to subsets of categories under MiFID.

Article 3(2) of CSDR requires that transferable securities traded on a trading venue within the meaning of MiFID II be recorded in book-entry form in a CSD. The objective is to ensure that those financial instruments can be settled in a securities settlement system, as those described by the Settlement Finality Directive (SFD). Recital 11 of CSDR indicates that CSDR does not prescribe any particular method for the initial book-entry recording. Therefore, in its advice, ESMA indicates that any technology, including DLT, could virtually be used, provided that this book-entry form is with an authorised CSD. However, ESMA underlines that there may be some national laws that could pose restrictions to the use of DLT for that purpose.

There may also be other potential obstacles stemming from CSDR. For instance, the provision of 'Delivery versus Payment' settlement in central bank money is a practice encouraged by CSDR. Where not practical and available, this settlement should take place in commercial bank money. This could make the settlement of securities through DLT difficult, as the CSDR would have to effect movements in its cash accounts at the same time as the delivery of securities on the DLT.

This section is seeking stakeholders' feedback on potential obstacles to the development of security tokens resulting from CSDR.

Question 88. Would you see any particular issue (legal, operational, technical) with applying the following definitions in a DLT environment?

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know / no opinion / strong concern
Definition of 'central securities depository' and whether platforms can be authorised as a CSD operating a securities settlement system which is designated under the SFD	○	○	◉	○	○	○
Definition of 'securities settlement system' and whether a DLT platform can be qualified as securities settlement system under the SFD	○	◉	○	○	○	○
Whether records on a DLT platform can be qualified as securities accounts and what can be qualified as credits and debits to such an account;	○	◉	○	○	○	○
Definition of 'book-entry form' and 'dematerialised form	○	◉	○	○	○	○
Definition of settlement (meaning the completion of a securities transaction where it is concluded with the aim of discharging the obligations of the parties to that transaction through the transfer of cash or securities, or both);	◉	○	○	○	○	○
What could constitute delivery versus payment in a DLT network, considering that the cash leg is not processed in the network	○	◉	○	○	○	○
What entity could qualify as a settlement internaliser	○	○	○	○	○	◉

Reasoning: The current (clearing and) settlement system has multiple functions, but presumably one of the main functions is to safeguard the proper settlement of a transaction in financial instruments and to limit counterparty risks by means of, among other things, the delivery-versus-payment system. We could imagine that full on chain trading, with crypto assets also being the payment methods, can embed an adequate transparent and immutable settlement system in itself. DVP with T+1 or even T+3 is not longer needed, because transactions settle instantly when upon a block of transactions being verified and accepted by the network on the basis of the applicable consensus protocol.

We do not see any issue in respect of definitions of financial instruments being in dematerialised form. Crypto assets will be in dematerialised form by nature. As to the definition of financial instruments being in book-entry form, this may require amendments to national laws in respect of book-entry securities transfers. From a Dutch law perspective, administering financial instruments in book-entry form results in those financial instruments to form a separate, segregated, capital from a Dutch legal perspective, ensuring that in the event of insolvency of the bank/custodian/intermediary where the financial instruments are deposited, those financial instruments in book-entry form fall outside the scope of the bankruptcy estate. It should be reviewed whether the Dutch

Securities (Bank Giro Transactions) Act (*Wet giraal effectenverkeer*) needs to be amended in order to provide sufficient legal certainty that crypto assets can be considered to be in book- entry form (and therefore form a legally separate capital) when administered/registered in a blockchain.

88.1 Is there any other particular issue with applying the following definitions in a DLT environment? Please specify which one(s) and explain your reasoning:

N/A; we would think that DLT can rather have advantages to the current settlement system instead of disadvantages.

Question 89. Do you consider that the book-entry requirements under CSDR are compatible with security tokens?

We would need to review this in more detail in order to share an opinion in this respect.

Question 90. Do you consider that national law (e.g. requirement for the transfer of ownership) or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT solution? Please explain your reasoning.

Under the current Dutch laws, the issuance and delivery of a share in the capital of a Dutch company requires a notarial deed. An exemption is made for the delivery of shares admitted to trading on a regulated market or MTF. A crypto asset reflecting, in the essence, a share in the capital of a Dutch company, is currently subjected to the normal transfer/delivery rules and such delivery therefore requires a notarial deed. It should be reviewed in more detail how Dutch civil law needs to be amended in order to ensure that any such transfer is legally valid if executed on a blockchain. The role of the notary is also one of a trusted third party. It should be assessed whether such role is still needed in case of equity interests being taken in Dutch companies in the form of crypto assets, issued and delivered on a blockchain. Taken the characteristics of a properly functioning blockchain (transparency, immutability), a 'shareholders register' on a blockchain could function as an adequate alternative to the current checks and balances performed by a Dutch civil law notary.

Question 91. Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment?

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know / no opinion / strong concern
Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system	◉	○	○	○	○	○
Rules on measures to prevent settlement fails	○	○	○	◉	○	○
Organisational requirements for CSDs	○	○	○	◉	○	○
Rules on outsourcing of services or activities to a third party	○	○	○	◉	○	○
Rules on communication procedures with market participants and other market infrastructures	○	○	○	◉	○	○
Rules on the protection of securities of participants and those of their clients	○	◉	○	○	○	○
Rules regarding the integrity of the issue and appropriate reconciliation measures	○	◉	○	○	○	○
Rules on cash settlement	○	○	○	○	○	◉
Rules on requirements for participation	○	○	○	◉	○	○
Rules on requirements for CSD links	○	○	○	○	○	◉
Rules on access between CSDs and access between a CSD and another market infrastructure	○	○	○	○	◉	○

Reasoning: Our main current concern is the legal uncertainty from a Dutch law perspective as to the validity of transfers of certain tokenized assets (such as shares or real property, for which a notarial deed is required) and the current lack of a clear framework applicable to crypto assets or, more generally, tokenized assets. Notaries, CSDs, clearing houses etc. are all trusted third parties and exist in order to minimize certain risks such as the counterparty risk. A proper functioning, robust blockchain could form a reliable alternative provided that the consensus protocol functions properly and that manipulation by one or some nodes working jointly is impossible.

91.1 Is there any other particular issue with applying the current rules in a DLT environment, (including other provisions of CSDR, national rules

applying the EU acquis, supervisory practices, interpretation, applications...)? Please specify which one(s) and explain your reasoning:

We would need to look into this in more detail to give valuable input.

Question 92. In your Member State, does your national law set out additional requirements to be taken into consideration, e.g. regarding the transfer of ownership (such as the requirements regarding the recording on an account with a custody account keeper outside a DLT environment)? Please explain your reasoning.

We defer to our answer to question 90. In addition thereto: the Dutch Securities (Bank Giro Transactions) Act (*Wet giraal effectenverkeer*) currently distinguishes a girodepot administered by a CSD (Euroclear Nederland in the Netherlands) and collective depots administered by admitted institutions/ intermediaries. The latter are banks and MiFID II licensed investment firms. From a Dutch law perspective, administering financial instruments in book-entry form requires these financial instruments to be initially issued/delivered to the holder of the depot (i.e. the CSD or an admitted institution/intermediary); legal title is held by such holder of the depot, whilst the investors merely hold the beneficial title of the financial instruments in book-entry form admitted to a girodepot or collective depot. This beneficial entitlement is in turn reflected by such investor's interest in the depot. We are not aware of any crypto assets being issued/delivered to a CSD or admitted institution/intermediary to be admitted to the depot held by such CSD or admitted institution

/intermediary at this stage. Therefore, we are not aware of any crypto assets currently being held in book- entry form, possibly caused by the absolute majority of crypto asset services providers currently not qualifying (or not properly being licensed as) an admitted institution/intermediary within the meaning of the Dutch Securities (Bank Giro Transactions) Act. We are aware of Euroclear Nederland, as CSD, looking into DLT and last year, they announced an end-to-end blockchain solution for commercial paper with certain partners (https://www.euroclear.com/newsandinsights/en/press/2019/2019_mr-11-Euroclear-developing- Blockchain-solution.html), but we do not have any knowledge of their experiences so far with this project nor of the manner in which this project is structured from a legal perspective. In any event, this project shows the interest as well as necessity to look into the applicability of the Dutch Securities (Bank Giro Transactions) Act to crypto assets.

9. The Alternative Investment Fund Directive

The Alternative Investment Fund Managers Directive (AIFMD) lays down the rules for the authorisation, ongoing operation and transparency of the managers of alternative investment funds (AIFMs) which manage and/or market alternative investment funds (AIFs) in the EU.

The following questions seek stakeholders' views on whether and to what extent the application of AIFMD to tokens could raise some challenges. For instance, AIFMD sets out an explicit obligation to appoint a depositary for each AIF. Fulfilling this requirement is a part of the AIFM authorisation and operation. The assets of the AIF shall be entrusted to the depositary for safekeeping. For crypto-assets that are not 'security tokens' (those which do not qualify as financial instruments), the rules for 'other assets' apply under the AIFMD. In such a case, the depositary needs to ensure the safekeeping (which involves verification of ownership and up-to-date recordkeeping) but not the custody. An uncertainty can arguably occur whether the depositary can perform this task for security tokens and also whether the safekeeping requirements can be complied with.

Question 105. Do the provisions of the EU AIFMD legal framework in the following areas are appropriately suited for the effective functioning of DLT solutions and the use of security tokens?

	1 (not suited)	2	3	4	5 (very suited)	Don't know / no opinion / very suited
AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;	○	○	◉	○	○	○
AIFMD provisions requiring AIFMs to maintain and operate effective organisational and administrative arrangements, including with respect to identifying, managing and monitoring the conflicts of interest;	○	○	○	◉	○	○
Employing liquidity management systems to monitor the liquidity risk of the AIF, conducting stress tests, under normal and exceptional liquidity conditions, and ensuring that the liquidity profile and the redemption policy are consistent;	○	◉	○	○	○	○
AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets;	○	○	○	○	○	◉
Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments.	○	○	○	◉	○	○

Reasoning: A distinction should be made between crypto funds (where the AIF's assets consist of crypto assets) and AIFs that issue crypto assets themselves as units/participation rights in the AIF for funding the fund assets. We limited our responses to the first category: where the AIF's assets are crypto assets. In our current view, we do not see a clear reason why depositaries cannot be appointed as safekeepers of an AIF's crypto assets in accordance with AIFMD; they could function as custodial wallet providers and hold the private keys to the AIF's crypto assets. Due to the volatility of crypto assets, the liquidity management of 'crypto asset AIFs' will, presumably, be more of a challenge and those rules need to be reviewed in detail in order to ensure that these can be applied by managers of 'crypto asset AIFs'.

Question 106. Do you consider that the effective functioning of DLT solutions and/or use of security tokens is limited or constrained by any of the AIFMD provisions?

We would need to look into this in more detail to give a valuable answer.

11. Other final comments and questions as regards tokens

It appears that permissioned blockchains and centralised platforms allow for the trade life cycle to be completed in a manner that might conceptually fit into the existing regulatory framework. However, it is also true that in theory trading in security tokens could also be organised using permissionless blockchains and decentralised platforms. Such novel ways of transacting in financial instruments might not fit into the existing regulatory framework as established by the EU acquis for financial markets.

Question 108. Do you think that the EU legislation should provide for more regulatory flexibility for stakeholders to develop trading and post-trading solutions using for example permissionless blockchain and decentralised platforms?

Yes. We defer to our prior answers, in particular those describing our ideas about introducing a 'base authorization/license requirement' (see questions 6, 14, 15, 24, 35.2, e.a.).

Question 109. Which benefits and risks do you see in enabling trading or post-trading processes to develop on permissionless blockchains and decentralised platforms?

We defer to our prior answers, in particular to questions 35-38 and 55-56.

Blockchain systems work in a fundamentally different way compared to the current trading and post-trading architecture. Tokens can be directly traded on blockchain and after the trade almost instantaneously settled following the validation of the transaction and its addition to the blockchain. Although existing EU acquis regulating trading and post-trading activities strives to be technologically neutral, existing regulation reflects a conceptualisation of how financial market currently operate, clearly separating the trading and post-trading phase of a trade life cycle. Therefore, trading and post-trading activities are governed by separate legislation which puts distinct requirements on trading and post-trading financial infrastructures.

Question 110. Do you think that the regulatory separation of trading and post-trading activities might prevent the development of alternative business models based on DLT that could more efficiently manage the trade life cycle?

No. As the length of this consultation document shows, there are multiple legal / regulatory concerns that need to be addressed in order to provide full legal certainty and a proper regulatory framework for all stakeholders in the crypto asset industry. We have no reason to believe, on the basis of our current information, that the regulation of trading and post-trading activities might have a hampering effect on the development of DLT business models. It is, however, questionable, whether any such separation will need to be upheld

/maintained if trading takes place on blockchains, taken the main characteristics of blockchains. In particular, if the NCAs are given certain rights on the relevant blockchain, the post trading reporting obligations as well as monitoring efforts may become much easier. We kindly defer to our prior answers (in particular to questions 55 and 56).

Question 111. Have you detected any issues beyond those raised in previous questions on specific provisions that would prevent effectively applying EU regulations to security tokens and transacting in a DLT environment, in particular as regards the objective of investor protection, financial stability and market integrity?

No, other than the issues that we have raised in our answers to this extensive consultation document, we currently have no particular additional concerns. In our view, it is very important that legal clarity is provided shortly, on a national, European and even on a global level.

We hold the view that most crypto assets can be brought under the existing regulatory framework, but note that we question whether this should be the way forward. We would be highly in favour of introducing a base authorisation/license requirement for starting financial undertakings, irrespective of whether they are active in the field of crypto assets or otherwise, subject to such authorisation regime providing a right balance between investor protection, financial stability, market integrity and proportionality for the crypto asset provider involved and which authorisation regime (and severity of requirements) grows with the undertaking on the basis of appropriate volume indicators. We favour this approach not just in relation to crypto asset providers but to any FinTech company or other start-up company offering financial services.

Furthermore, in our view, back end systems making use of DLT and crypto assets to facilitate a speedy and more robust back end administrative system should be excluded from a regulatory framework as long as such crypto assets are not meant to be used in such manner by front end users.

Lastly, national laws should be reviewed and, where needed, amended in order to take away any legal concerns and legal uncertainty in respect of the validity of issuance, transfers/delivery etc. or crypto assets.

Question 112. Have you identified national provisions in your jurisdictions that would limit and/or constraint the effective functioning of DLT solutions or the use of security tokens?

Yes. We defer to our answers to questions 90-91.

C. Assessment of legislation for 'e-money' tokens

Electronic money (e-money) is a digital alternative to cash. It allows users to make cashless payments with money stored on a card or a phone, or over the internet. The e-money directive (EMD2) sets out the rules for the business practices and supervision of e-money institutions.

In its advice on crypto-assets, the EBA noted that national competent authorities reported a handful of cases where payment tokens could qualify as e-money, e.g. tokens pegged to a given currency and redeemable at par value at any time. Even though such cases may seem limited, there is merit in ensuring whether the existing rules are suitable for these tokens. In that this section, payments tokens, and more precisely "stablecoins", that qualify as e-money are called 'e-money tokens' for the purpose of this consultation. Consequently, firms issuing such e-money tokens should ensure they have the relevant authorisations and follow requirements under EMD2.

Beyond EMD2, payment services related to e-money tokens would also be covered by the Payment Services Directive (PSD2). PSD2 puts in place comprehensive rules for payment services, and payment transactions. In particular, the Directive sets out rules concerning a) strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud; b) the transparency of conditions and information requirements for payment services; c) the rights and obligations of users and providers of payment services.

The purpose of the following questions is to seek stakeholders' views on the issues they could identify for the application of the existing regulatory framework to e-money tokens.

Question 113. Have you detected any issue in EMD2 that could constitute impediments to the effective functioning and/or use of e-money tokens?

We agree that stablecoins could qualify as electronic money, or if you will e-money tokens. Upon those tokens qualifying as e-money, indeed all payment services provided in respect of such e-money tokens, could fall under PSD2. We defer to our answers to questions 25 and 35.2. In any event, to prevent regulatory arbitrage, clarity as to the applicability of these EU Directives should be provided on an EU level.

One issue could arise with the requirements applicable to the funds deposited with the 'e-token issuer' to be exchanged into e-money tokens. Currently companies active in the field of crypto assets are practically barred by banks and have difficulty opening a bank account. The funds received for exchange in e-money tokens must be segregated from the EMI and e.g. deposited on a separate bank account. How can they do that if they are not offered bank accounts? The current reluctance of banks to accept any crypto asset service provider is, to our understanding, mainly based on AML/CFT reasons. AMLD V should already bring some relieve to that end. However, we expect that more clarity in respect of the regulatory framework applicable to crypto asset service providers, including those involved in stablecoins, would have a positive impact on the development of these types of business models and, subject to such crypto asset service providers having obtained the relevant authorisations, to have a positive effect on the willingness of the banks to accept these types of clients as well.

Question 114. Have you detected any issue in PSD2 which would constitute impediments to the effective functioning or use of payment transactions related to e-money token?

See answer to 113. Furthermore, the new payment services (account information services and payment initiation services) may need to be reviewed in light of any blockchain applications offering services for e- money tokens (or any other crypto asset that could qualify as a fund within the meaning of PSD2). Would an application that offers information in respect of e.g. multiple crypto wallets holding e-money tokens qualify as an AISP resulting in (in the Netherlands) a license requirement (and without having the possibility to rely on an exemption which would be available to 'small' PSPs offering payment services 1-5 in respect of e-money tokens? Would that be proportionate?)? Furthermore, would a custodial wallet provider with a mandate from its client to authorise or conduct any transactions involving e-money tokens be considered a PISP, resulting in a license requirement (and again not being able to rely on an exemption which would be available to 'small' PSPs as

described above)? Is such a custodial wallet provider - other than 'normal' PISPs - considered to actually hold e-money tokens on behalf of its clients, and therefore funds within the meaning of PSD2, resulting in the potential necessity to the rules around separation of assets to be reviewed?

Question 115. In your view, do EMD2 or PSD2 require legal amendments and /or supervisory guidance (or other non-legislative actions) to ensure the effective functioning and use of e-money tokens?

Yes. See our answers to 113 and 114.

Under EMD 2, electronic money means "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions [...], and which is accepted by a natural or legal person other than the electronic money issuer". As some "stablecoins" with global reach (the so-called "global stablecoin") may qualify as e-money, the requirements under EMD2 would apply. Entities in a "global stablecoins" arrangement (that qualify as e-money under EMD2) could also be subject to the provisions of PSD2. The following questions aim to determine whether the EMD2 and/or PSD2 requirements would be fit for purpose for such "global stablecoins" arrangements that could pose systemic risks.

116.1 Is there any other requirement under EMD2 that would be appropriate for "global stablecoins"? Please specify which one(s) and explain your reasoning:

We would need to review EMD2 in detail in order to be able to give valuable feedback in this respect. It is of the essence that issuers of stablecoins, irrespective of whether these are global stablecoins or not, can uphold the underlying asset value to which the stablecoin is pegged / the value that it represents. The capital requirements (and other regulatory requirements) surrounding such forms of crypto assets should be proportionate to the pegged asset value at all times. Also in this respect we opt for a regulatory framework that growth with the company, offering sufficient safeguards and investor protection, but preventing the potential hampering of this type of developments due to a full EMD2, PSD2 or alike regulatory framework becoming applicable immediately upon such undertaking commencing its business.

Question 117. Do you think that the current requirements under PSD2 which are applicable to e-money tokens are appropriate for "global stablecoins" (i.e. those that reach global reach)?

We defer to our answer to question116.1. We would need to review PSD2 in detail in order to be able to give valuable feedback in this respect.