EUROPEAN COMMISSION
Directorate-General for Financial Stability, Financial Services and Capital Markets Union

CONSULTATION DOCUMENT

On an EU framework for markets in crypto-assets

Disclaimer

This document is a working document of the Commission services for consultation and does not prejudge the final decision that the Commission may take.

The views reflected on this consultation paper provide an identification on the approach the Commission services may take but do not constitute a final policy position or a formal proposal by the European Commission.

You are invited to reply by **19 March 2020** at the latest to the online questionnaire available on the following webpage:

https://ec.europa.eu/info/publications/finance-consultations-2019-crypto-assets_en

Please note that in order to ensure a fair and transparent consultation process **only responses received through the online questionnaire will be taken into account and included in the report summarising the responses.**

This consultation follows the normal rules of the European Commission for public consultations. Responses will be published unless respondents indicate otherwise in the online questionnaire.

Responses authorised for publication will be published on the following webpage:

https://ec.europa.eu/info/publications/finance-consultations-2019-crypto-

assets_en

PUBLIC CONSULTATION

I. Questions for the general public

As explained above, these general questions aim at understanding the EU citizens' views on their use or potential use of crypto-assets.

1) **Have you ever held crypto-assets?**
   - **Yes**
   - **No**

2) **If you held crypto-assets, what was your experience?**

   1.1. Was it simple and straightforward to buy them?

   - **simple**
   - **neither easy nor hard**
   - **complex**

   1.2. Did you feel sufficiently well informed about your rights, the risks and opportunities?
   - **Yes**
   - **No**

   1.3. Did you buy the crypto-assets from an EU or non-EU vendor, exchange or trading platform?
   - **EU**
   - **Non-EU**
   - **Don't know**

   1.4. Did you hold the crypto-assets with a custodial wallet provider?
   - **Yes**

- **No**

1.5. What type of crypto-assets, have you held?

- **Crypto-assets backed by assets (such as cash, gold, shares, bonds, or other real world assets…)**
- **Payment tokens/virtual currencies (such as bitcoin)**
- **Crypto-assets giving the right to use a service or access a product**
- **Other**

1.6. Did you make any profit or a loss on the crypto-assets you held?

- **Profit**
- **Loss**
- **I was able to use them for the services or products promised**
- **Other**

1.7. Have you experienced any loss as a result of safekeeping issues with your crypto-assets?

- **Yes**
- **No**

3) Do you plan or expect to hold crypto-assets in the future?

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain the reasons why you are planning to hold crypto-assets (if needed).

4) If yes, in what timeframe?

- **in the coming year**
- **2-3 years**
- **more than 3 years**

II. Classification of crypto-assets[1]

There is not a single widely agreed definition of 'crypto-asset'. 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'*[2] 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

[1] 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.

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

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.

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**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

This would depend on the definitions. The definition that this consultation uses for a crypto asset includes a reference that it would exist on a digital ledger. However, there are also crypto or digital assets that are not necessarily based on a digital ledger (of which it is unknown that they are). A more functional or activity based approach, which is technology agnostic, would be more useful. This would mean that when either a crypto or digital asset provides a function that could be labelled as a financial service, it should be taken within scope.

6) **In your view, would it be useful to create a classification of crypto-assets at EU level?**

- **Yes**
- **No**
- **Don't know/no opinion**

If yes, please indicate the best way to achieve this classification (non-legislative guidance, regulatory classification, a combination of both…). Please explain your reasoning.

Yes, a classification based on a functional perspective may help understand the various forms of crypto assets that have emerged over the past few years, and would lead to a more harmonized approach among member states.

As mentioned before, we are hesitant towards a classification of crypto assets that relies too much on technicality rather than functionality, since the former is always a mere snapshot of the current state of innovation and can change. By classifying the ecosystem based on its current technical state, incumbents may enjoy regulatory advantages over those that want to drive innovation. Instead, we strongly advocate to develop a broad and coarse classification that assesses utility, function and impact rather than the underlying technology. However, definitions of what constitutes a financial asset are already available and do not necessarily require changes as they are supposed to be technology neutral.

The best way to clarify certain definitions would depend on the follow up of this consultation. If a specific crypto and/or digital asset framework were to be considered, it would make sense to use a regulatory classification with relevant references to the existing EU frameworks because some tokens / assets have functions already incorporated in EU rules (for instance investment tokens). Another possibility would be that the ESA's issue a common, EU-wide taxonomy to be used by the NCA's.

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).**

In general, we have identified three main types of crypto assets (also referred to as tokens) in general:

1) Transaction token:

These are used as a means for general transactions of value transfers (without implying that they are an alternative to fiat currency), and can be used to execute global peer-to-peer transactions without the involvement of a third party (such as a bank or money transfer business). Depending on the exact characteristics of these token, they may or may not fall within the scope of existing payments regulations.

2) Utility crypto token:

These can be seen as the entitlement to the use of, or access to, a specific application or service offered by or through a provider's platform (either DLT-based or not).

3) Investment token:

These are used as an alternative for, or addition to, existing financial instruments. This type of crypto asset may or may not qualify as a financial instrument as defined by MiFID II and the Dutch Financial Supervision Act (Wet op het financieel toezicht, Wft). Some represent, for example, shares, bonds or units in an investment fund. Others share similarities with (legally defined) financial instruments or regulated activities, but are legally constructed in such a way that prevents them to be qualifying as financial instruments, making them fall outside of the scope of financial supervision, while de facto having the same characteristics as financial instruments.

A fourth type of token, the protocol token, could potentially be considered as a distinctive crypto asset. Most blockchains use tokens to compensate for certain activities in the maintenance of the network (mining, for example). These have been referred to as protocol tokens, as they anchor complex incentive mechanisms in the protocol governing the network's maintenance (see for example: L. Perlman: Regulation of the Financial components of the Crypto-economy, p. 142.).

The division between transaction tokens, utility tokens and investment tokens (and potentially protocol tokens) is a useful perspective that enables a preliminary distinction on functionality. However, it should be noted that individual crypto assets are not limited to one of the abovementioned types, making them potentially hybrid. That said, within a specific timeframe in most cases one of these types dominates (and relevant rules should apply accordingly).

Furthermore, the emergence of so-called stablecoins has challenged this distinction in various ways, as these do not necessarily pertain to a certain activity, but rather a type of (centralized) system where certain activities that in the governance of a fiat currency are performed by public institutions (such as a central bank), are performed by private parties. Defining a so-called stablecoin can be difficult, as they can be used for different types of activities, and have a different scope regarding use and potential users. Furthermore, the name "stablecoin" is deceitful as many of these crypto assets are not as stable as they claim to be, so a new technical term might be useful.

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'?**

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed). If yes, indicate if any further sub-classification would be necessary.

As mentioned in the answer to question 6, a common (broad) taxonomy of different functionalities of crypto assets can be useful. The three categories of utility, investment, and transaction tokens could provide such an outline. We would prefer to use the term transaction token, rather than payment token, as such tokens are not necessarily only used for payments, and could furthermore infer that they, per definition, are subject to existing payments regulations.

However, we do like to stress that regulators should refrain from creating new legal categories whenever a new type of asset is encountered, and/or putting them in the "hybrid tokens" basket. Instead, regulators should assess the functionality or impact of a given individual asset, and be aware that these are of a transient nature. Therefore it is better not to speak of a separate type of 'hybrid tokens', but to realize that, as by default, the sector itself is continuously innovating and developing, and new types of tokens can arise in the coming years.

The Deposit Guarantee Scheme Directive[3] (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.

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?**

A crypto-asset itself cannot be a 'deposit', since it is not a claim, but an asset in itself. But a crypto-asset could represent a deposit or claim by having a deposit or claim attached to it which is transferred along with the asset.

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

[3] Deposit Guarantee Schemes Directive (2014/49/EU)

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[4] (**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-asset sector (**C.**).

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.

10) In your opinion, what is the importance of each of the potential benefits related to crypto-assets listed below? Please rate each proposal from 1 to 5, 1 standing for "not important at all" and 5 for "very important".

	1	2	3	4	5	No opinion
Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs				X		
Issuance of utility tokens as an alternative funding source for start-ups				X		
Cheap, fast and swift payment instrument				X		
Enhanced financial inclusion			X			
Crypto-assets as a new investment opportunity for investors			X			
Improved transparency and traceability of transactions			X			
Enhanced innovation and competition				X		
Improved liquidity and tradability of tokenised 'assets'						X
Enhanced operational resilience (including cyber resilience)			X			
Security and management of personal data	X					
Possibility of using tokenisation to coordinate social innovation or decentralised governance						X
Other						

[4] 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)

Please justify your reasoning (if needed).

Our own definition of a utility token seems to differ from the one that is used in the first and second row. Where the table mentions utility tokens, we would consider them investment tokens.

We recognise the potential of crypto assets to a cheaper, faster and more accessible payment system, although this potential might be limited in the EU since instant payments have already created a very fast and reliable payment system in the SEPA. Nevertheless, global reach and financial inclusion are areas where growth may still be achieved.

We see potential for the technology behind crypto's, such as blockchain or (more generally) distributed ledger technology (DLT), as well as smart contracts in various areas. Of particular interest are those areas where this technology is applied to improve internal business operations. When used appropriately, the technology may be used to improve performance and reduce risk without exposure to financial or market (e.g. trading) risk.

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[5]. 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[6]. 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[7], this might change in the future.

11) In your opinion, what are the most important risks related to crypto-assets? Please rate each proposal from 1 to 5, 1 standing for "not important at all" and 5 for "very important".

	1	2	3	4	5	No opinion
Fraudulent activities					X	
Market integrity (e.g. price, volume manipulation…)					X	
Investor/consumer protection					X	
Anti-money laundering and CFT issues					X	
Data protection issues				X		
Competition issues				X		
Cyber security and operational risks				X		
Taxation issues			X			
Energy consumption entailed in crypto-asset activities				X		
Financial stability		X				

[5] ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019

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

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

Monetary sovereignty/monetary policy transmission		X				
Other						

Please justify your reasoning (if needed).

Fraudulent activities with crypto assets and manipulation rates are extremely high. Please find some illustrations below:

- For a summary of hacks, see Cermak, L (2019) Research: Cryptocurrency exchange hack surpass $1.3 billion all time; 61% coming from 2018.
- The ICO market has sharply fallen, notably only between 25%-33% of crypto-assets issued through ICOs during the course of 2017-2018 are currently being traded. Of 5489 published ICOs, 3400 did not raise funds. See ICO Bench (2019) ICO Market Report for more information.
- A common problem with the current 'Nakamoto' consensus-based systems, are called 51% attacks and selfish mining attacks. A malicious actor by accumulating 51% of mining power can conduct a double spend attack and so threaten the health of the system by allowing the possibility for blocks to be revoked. Arbitrageurs may find it financially attractive to rent hashing power in order to perform these attacks.
- The amount of stolen crypto-currency from exchanges in 2018 has been reported at USD 2.7 million in crypto assets stolen every day, or USD 1,860 each minute.
- Data may be inflated through 'wash trading' and unsophisticated reporting tools, with one report submitted to the US SEC in March 2019 claiming that some 95% of all reported Bitcoin trading volume is either fake volume or wash-trading (see CryptoHype (2018) Cryptocurrency Exchanges engaging in High-level Wash Trading to fake Trade volumes).

Regarding AML/CFT, multiple national and international organisations, including the UN Security Council, FATF, G20 and Europol have mentioned the risks that crypto assets pose to money laundering and the financing of terrorism. Some recent cases of the Dutch criminal investigation authorities underline these risks, for example: https://www.fiod.nl/the-fiod-and-the-public-prosecution-service-take-money-laundering-machine-for-cryptocurrencies-offline/

In terms of data protection, there are concerns about the general availability of transaction data to the public, as many (distributed) blockchains and related crypto assets only offer a certain type of pseudonymity. This draws the question whether these applications and projects are GDPR-proof.

Regarding competition issues one could argue that crypto assets can be used to create more choices for consumers and businesses, and that the innovation that these new assets offer incentives to existing financial parties to improve their proposition. On the other hand, certain crypto asset projects, especially some stablecoin proposals, involve major multinational companies that already have important positions of power when it comes to data, and could potentially lead to unfavorable positions of market dominance.

When the main objective of the technology is to enable cheaper, faster and more reliable payments, and when businesses use it for that purpose, this development can still allow for effective monetary policy transmission and financial stability. On the other hand, due to the anonymous nature and technical complexity, the risk of fraud, market manipulation and money-laundering remains high. This is confirmed by the reality we are in, as we have observed various cases of the latter, but not the former.

This status quo is only likely to change in the case of mass adoption. This does have implications to financial stability and monetary policy transmission which need to be addressed with tailored regulatory solutions. A new regulatory proposal should address these aspects of crypto-assets when they apply.

"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*'[8] 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).

12) In our view, what are the benefits of "stablecoins" and "global stablecoins"? Please explain your reasoning (if needed).

The emergence of so-called (global) stablecoins provides opportunities for making payments faster and more efficient. Cross-border payments in particular still tend to be costly, complex and slow. "Wholesale" stablecoins could be of use in transactions between financial institutions, decreasing the need for correspondent banking and therefore making cross-border payments cheaper and faster.

13) In your opinion, what are the most important risks related to "stablecoins"? Please rate each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".

	1	2	3	4	5	No opinion
Fraudulent activities				X		
Market integrity (e.g. price, volume manipulation…)				X		
Investor/consumer protection					X	
Anti-money laundering and CFT issues				X		
Data protection issues					X	
Competition issues					X	
Cyber security and operational risks					X	
Taxation issues			X			
Energy consumption			X			
Financial stability					X	
Monetary sovereignty/monetary policy transmission					X	
Other						

Please explain in your answer potential differences in terms of risks between "stablecoins" and "global stablecoins" (if needed).

[8] G7 Working group on 'Stablecoins', Report on 'Investigating the impact of global stablecoins', October 2019

The difference between global and non-global stablecoins pertain especially to risks with regard to financial stability, monetary sovereignty/monetary policy transmission. Also with regard to investor/consumer protection, and cyber security and operational risks, these become more urgent as a stablecoin has the potential to evolve into a global stablecoin (or is introduced as a global stablecoin, for example by a “bigtech” company). In other words: when a stablecoin has the potential to become systemically important (e.g. impacting the real economy), the risks grow.

Other risks such as money laundering or market abuse and fraud can also increase in the case of global reach, for instance when mass-adoption makes it easier to achieve anonymity or deploy fraud schemes.

Data protection and competition risks arise when large private parties, which already have a dominant market position with regards to data, introduce their own stablecoin. The availability of transaction data might reinforce their dominant market position and lock-in customers even more. Furthermore, supervision in terms of data protection when another stream of personal data is introduced in these companies might become more difficult.

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.

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**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

A bespoke regime for crypto assets, especially those that do not do not immediately qualify as an existing financial service or instrument, helps to achieve a level playing field which encourages innovation and growth, and could mitigate certain specific risks. Current existing regulations, such as EMD2 or PSD2, have not been created with crypto assets in mind. In trying to fit new businesses under an existing regulatory framework, there is a risk of putting them at a disadvantage when they do not fit the type for which it was intended, or unintendedly create unwanted legal loopholes. The possibility of global stablecoins has made this call for a bespoke regime more pressing than it was before, as the market of crypto-assets is of relatively low volume.

However, a balance must be struck, and a "same product, same risks, same rules" approach is important. Those crypto assets that qualify (or are practically the same) as existing regulated activities and/or instruments must be treated as such, in order to avoid regulatory arbitrage. This would, for example, also include investment tokens that legally might not qualify as a financial instrument, but in practice perform the same function and offer the same rights (e.g. a tokenized share). Therefore, a bespoke regime should cover those crypto assets that are currently clearly not regulated.

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.

As of now, the only (financial) legislation in the Netherlands that has specifically been drafted with crypto assets in mind has been the revised fourth anti-money laundering directive (directive (EU) 2018/843). Futhermore, non-financial regulation of crypto assets has also been introduced with the directive on combating fraud and counterfeiting of non-cash means of payment (Directive (EU) 2019/713). The implementation of both directives into Dutch law is currently ongoing. No other national financial legislation that specifically targets crypto assets is in place in The Netherlands. This does not mean that crypto assets are not covered by other types of legislation, such as criminal, sanctions and civil law. The Dutch government has recently published a report on the legal aspects of the use of blockchain and DLT in The Netherlands, in which more clarity is given on the different types of legislation that might cover transactions on a blockchain (only in Dutch via: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/12/17/tk-kabinetsreactie-op-het-verkennende-onderzoek-blockchain-en-het-recht).

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)

The goal of a bespoke crypto-regime should be to foster innovation and a healthy business environment for growth, while adequately mitigating the above mentioned risks, including to financial stability at the same time. We should prevent situations of regulatory arbitrage where businesses willingly and knowingly structure their business outside the scope of a given regime. Therefore a regime for crypto assets should focus on the functionality of the different assets, and not pre-emptively exclude certain types (such as stablecoins) from their scope from the outset. However, if after thorough deliberation it is understood that a specific activity or functionality need not to be regulated further, it might be excluded.

17) **Do you think that the use of crypto-assets in the EU would be facilitated by greater clarity as to the prudential treatment of financial institutions' exposures to crypto-assets[9]?**

- **Yes**
- **No**
- **Don't know/no opinion**

Please indicate how this clarity should be provided (guidance, EU legislation…).

Possibly. We think the Basel paper mentioned in footnote 26 provides useful suggestions for a prudential framework for credit institutions who are involved in crypto assets.

18) **Should harmonisation of national civil laws be considered to provide clarity on the legal validity of token transfers and the tokenization of tangible (material) assets?**

Clarity on the legal validity of digitized token transfers and the definition/categorisation of tokenization of tangible (material) assets is desirable, for both tokenized assets in a permissioned- and permissionless blockchain environment. However, the necessity for harmonized (civil) legislation at European level has not been established yet. Experiences in the Netherlands show that unfamiliarity with the possibilities within existing legislation or unfamiliarity with the interpretation of existing legislation can often lead to the impression that there are blockades in legislation or that there is insufficiently harmonized legislation. It is therefore advisable to conduct thorough research at the European level into the possibilities that existing legislation offers before deciding to amend existing regulations.

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

[9] See the discussion paper of the Basel Committee on Banking Supervision (BCBS) "Designing a prudential treatment for crypto-assets", December 2019

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.

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?

Current estimates

Around 50-100 crypto service providers are present in the Netherlands. Their activities concern services like exchange platforms, crypto money machines (ATMs), traders and custodial wallet providers

Estimates December 2018

Research by the AFM and DNB shows that about 40 crypto service providers were established in the Netherlands in October 2018, including central exchange platforms, crypto money machines (ATMs), traders and wallet providers. The majority offers exchange services in the form of trading for their own account, possibly via cryptocards. A number of providers offer saving functions too. Around 10 providers of cryptocards are operational in the Netherlands. Two central exchange platforms, on which customers can trade certain cryptos with each other and exchange them for euros, are established in the Netherlands. The daily traded volumes in Bitcoin on the estimated largest Dutch platform are 0.01% of the total traded worldwide volume in Bitcoin in euros.

There is not a specific number of ICOs offered from the Netherlands. On the basis of the available information, it can be concluded that the supply is limited. There are approximately 98 Dutch ICOs known from 2017 to November 2018 compared to around 4,600 ICOs worldwide in this period. After the popularity point of cryptos in January 2018, it appears providers of ICOs in the Netherlands have difficulties raising capital: whereas early in 2018 ICOs reported that they had achieved their intended capital targets in a few weeks, this is hardly the case for the later issued ICOs. Additionally, at the InnovationHub of the AFM and DNB, the providers of (potential) ICOs indicate that consumer interest has decreased sharply during 2018.

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[10]. 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

[10] Study from the European Parliament on “Cryptocurrencies and Blockchain”, July 2018

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.

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?**

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

In our view, every exchange or wallet provider should have an office in the EU to provide services to EU customers, and furthermore be licensed in the host country. We have already introduced these requirements in the national implementation of AMLD5, as, in our interpretation of AMLD5, this is required in order to be able to supervise these entities properly. Depending of the functionality of the token, this is not the case for the inventor or issuer of the crypto. If an issuer or sponsor will be regulated by EU law, we think the same rules should apply as currently apply on the exchange and wallet provider, which means that a physical presence in the EU is required. If an issuer or sponsor is not regulated by EU law and offers directly to consumers/investors in the EU, we think it would be preferable that the issuer/sponsor has a physical presence in the EU.

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?**

- **Yes**
- **No**
- **This depends on the nature of the crypto-asset (utility token, payment token, hybrid token…)**
- **Don't know/no opinion**

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…).

Ideally, everything that is sold commercially is accompanied by a proper description. For the sake of financial regulation we believe that crypto assets that have a financial function or components similar to financial activities/functions that are currently regulated, should fall under similar requirements. For investment tokens, regimes like PD, crowdfunding and AIFMD are very relevant.

Requiring an issuer or sponsor to produce a 'white paper' puts great responsibility on the consumers too, for they may be legally disadvantaged, especially when consumers do not have the technical knowledge to read and understand it. It is more important for the issuer or, more generally, the crypto asset service provider to explain what their business does in terms of functionality and utility, as well as to give an account of the amount of exposure a client has to certain (volatile) assets.

Taking in consideration that crypto assets are complex products, a financial disclosure must be a requirement.

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)? Please rate each proposal from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".**

	1	2	3	4	5	No opinion
The Consumer Rights Directive[11]					X	
The E-Commerce Directive[12]				X		
The EU Distance Marketing of Consumer Financial Services Directive[13]					X	
Other (please specify)						

Please explain your reasoning and indicate the type of clarification (legislative/non legislative) that would be required

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? Please rate each proposal from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant ".**

	1	2	3	4	5	No opinion
The managers of the issuer or sponsor should be subject to fitness and probity standards					X	
The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions					X	

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					X	
Other					X	

Please explain your reasoning (if needed).

This would be in line with current rules on selling / advertising products and services.

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).

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 (if needed).

The attribute 'global' refers to a stablecoin with a potential global reach and adoption across multiple jurisdictions worldwide and the potential to achieve substantial volume, rather than a specific legal or regulatory concept. However, none of the existing operational stablecoins currently appear to have reached a global scale (yet). Also no objective criteria have been agreed upon on an international level to distinct between 'normal' and 'global' stablecoins.

Therefore, in this point of time, we believe stablecoin initiatives should be assessed whether they have the potential to be used more widely (e.g. within several jurisdictions) as a means of payment, a store of value and/ or widely as substitute for domestic currency. In other words, when a stablecoin initiative has the potential to become systemically important, including through the substitution of domestic currencies, then we believe it should be regarded as 'global' stablecoin.

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? Please indicate for <u>both "stablecoins" and "global stablecoins"</u> if each is proposal is relevant (leave it blank if you have no opinion).

	"Stablecoins"		"Global stablecoins"	
	Relevant	**Not relevant**	**Relevant**	**Not relevant**
The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds…)			X	
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			X	
The assets or funds of the reserve should be segregated from the issuer's balance sheet	X		X	
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	X		X	
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	X		X	
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	X		X	
Obligation for the assets or funds to be held in custody with credit institutions in the EU			X	
Periodic independent auditing of the assets or funds held in the reserve	X		X	
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	X		X	
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	X		X	
Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer		X	X	
Other				

Please illustrate your response (if needed).

When a specific stablecoin could potentially evolve into a global stablecoin (or is introduced as global stablecoin, by a bigtech for example), all of the abovementioned requirements are relevant for its issuer(s) and/or the manager(s) of the reserve.

However, for other stablecoins that are, for example, backed by other crypto assets, we believe that not all of above mentioned requirements are completely relevant, as long as those stablecoins do not have the intention, nor the potential, to become systemically important (i.e. impacting the real economy by becoming a widely used means of payment, a store of value and/ or used widely as substitute for domestic currency).

"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".*

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**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

We agree with the mentioned G7 report that the risks regarding wholesale and retail (and potentially global) stablecoins are of a different nature and require different regulatory and supervisory treatments. It is also in line with our view that we should take an activity-based approach to regulating crypto assets, and look at functionalities.

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 venues[14] while others use simple and inexpensive technology.

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

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? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Absence of accountable entity in the EU					X	
Lack of adequate governance arrangements, including operational resilience and ICT security				X		
Absence or inadequate segregation of assets held on the behalf of clients (e.g. for 'centralised platforms')				X		
Conflicts of interest arising from other activities					X	
Absence/inadequate recordkeeping of transactions					X	
Absence/inadequate complaints or redress procedures are in place					X	
Bankruptcy of the trading platform					X	
Lacks of resources to effectively conduct its activities				X		
Losses of users' crypto-assets through theft or hacking (cyber risks)				X		
Lack of procedures to ensure fair and orderly trading				X		
Access to the trading platform is not provided in an undiscriminating way					X	
Delays in the processing of transactions					X	
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)				X		
Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse					X	
Other					X	

Please explain your reasoning (if needed).

Some of the operational risks listed above, such as inadequate recordkeeping of transactions, are the problem that certain crypto-assets are trying to solve rather than create. It is this aspect of blockchain technology that we embrace and which development should be fostered by a well-suited regulatory framework. Yet trading platforms also introduce new risks, for example when they do not provide enough transparency with regards to the financial risks of their customers.

Rules & Regulations
If crypto assets represent a financial instrument and is tradable on a venue, the same rules and regulations of venue trading of financial instruments should apply, e.g. to maintain a level playing field. For hybrid crypto assets a clarification of the applicable legal requirements should be provided, aiming for the same outcome if the asset would not have been digital.

Background information on the functions of platforms and associated risks

- Accountability & Responsibility
  Accountability in public distributed ledgers remains challenging. Control over and system availability of IT-infrastructure of the digital asset used should primarily be a responsibility of the relevant trading platform. Crypto-trading platforms usually perform all traditional roles, e.g. trading venue, clearing, settlement and CSD-like roles.
- Key management & conflicts of interest
  Centralized platforms require users to deposit their assets with the platform prior to trading. In the crypto-asset world, this means providing the exchange with their private keys. Additionally, fiat money must be deposited to pay for any fiat-crypto pairings. Often these are fungible; users do not see their wallets housed in the exchange, but the wallet balance is a database entry updated by the exchange itself, where all the funds in the exchange are commingled (quite regularly with exchange's own funds). Thus, the exchange is responsible for keeping the records of ownership. It is impossible for an outside auditor or party to verify this in the absence of mandatory regulations.
- Cyber-security
  Cyber-security is a greater challenge in public DLTs without permissions because there are no walled gardens, which only allow access to known, trusted participants. So everyone has access, but no one can be trusted. So despite the use of strong cryptography, DLTs are not necessarily a panacea for security concerns.
- No accuracy check on data input
  Although the data on a blockchain is said to be secure, and any block additions approved by consensus, the blockchain cannot address the reliability or accuracy of the data input. Not with the current technology: a blockchain addresses a record's authenticity by confirming the party or parties submitting a record, the time and date of its submission, and the contents of the record at the time of submission, and not the reliability or accuracy of the records contained in the blockchain.
- Blockchain application become outdated by 2021
  Most exchange-based trading is done off-chain, with settlement done on-chain. Because of the current technology constraints, this is notoriously slow. There are concerns on the longevity of DLTs too. Contingencies to rescue data on obsolete DLTs must be devised. A Gartner report warned that 90% of blockchain technology used by enterprises in 2019 risk becoming obsolete or insecure by 2021, because of fragmentation and lack of interoperability. https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain
- Counterparty Risk
  As current crypto trading platforms are clearinghouses and settlement institutions simultaneously, the model leads to illiquid markets as one needs to differ between clearing and settlement.
- Speed & Scalability
  The imperfections of blockchain are often illustrated by the blockchain trilemma (security, governance and scalability), introduced by Ethereum founder Vitalik Buterin. The blockchain scalability trilemma represents a widely held belief that the use of blockchain presents a tri-directional compromise in efforts to increase scalability, security and decentralization. Looking at this from a crypto-economy a new element arises: liquidity (which constitutes a new trilemma: security, scalability and liquidity).

For more information please find the following research:

- L. Perlman: 'Regulation of the financial Components of the Crypto-Economy'. https://sipa.columbia.edu/sites/default/files/25222_SIPA-White-Paper-CE-Regulation-web.pdf
- A.S. Kavuri and A. Milne: 'Evolution or revolution? Distributed ledger technologies in financial services.' https://crawford.anu.edu.au/sites/default/files/publication/cama_crawford_anu_edu_au/2020-01/4_2020_kavuri_milne.pdf
- DTCC: Guiding principles for the post-trade processing of tokenized securities. file:///U:/Downloads/Crypto-Asset-Whitepaper-2019.pdf
- Greenwich: Steampunk Settlement: deploying futuristic technology to achieve an anachronistic result. https://www.greenwich.com/steampunk-settlement-report-download

28) What are the requirements that could be imposed on trading platforms in order to mitigate those risks? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Trading platforms should have a physical presence in the EU					X	
Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					X	
Trading platforms should segregate the assets of users from those held on own account					X	
Trading platforms should be subject to rules on conflicts of interest					X	
Trading platforms should be required to keep appropriate records of users' transactions					X	
Trading platforms should have an adequate complaints handling and redress procedures					X	
Trading platforms should be subject to prudential requirements (including capital requirements)				X		
Trading platforms should have adequate rules to ensure fair and orderly trading					X	
Trading platforms should provide access to its services in an undiscriminating way					X	
Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse					X	
Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)					X	
Trading platforms should be responsible for screening crypto-assets against the risk of fraud					X	
Other					X	

Please indicate if those requirements should be different depending on the type of crypto-assets traded on the platform and explain your reasoning (if needed).

Depending whether the asset that is traded qualifies as a financial instrument under MiFID II, trading these assets should be in accordance with those rules (and of associated legislation). However, these rules need not necessarily be applied to the trade of tokens that do not qualify as a financial instrument.

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[15].

29) In your opinion, what are the main risks in relation to crypto-to-crypto and fiat–to-crypto exchanges? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

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

Please explain your reasoning (if needed).

An important aspect of regulation is stimulation and promotion of sustainable forms of innovation. If a crypto asset can be considered as a financial instrument, such exchanges are equal to investment firms or trading venues and therefore financial regulation applies. If existing practices regarding exchanges are corrected, regulation must not apply; crypto assets are very seldom used for payments.

The risk depend on the different business models of exchanges, and the specific type of transactions that they safeguard. The point where the cryptos enter the traditional financial system, AML and CFT risks arise. Because of this responsibility, exchanges have become gatekeepers to the financial system with the introduction of AMLD5.

30) What are the requirements that could be imposed on exchanges in order to mitigate those risks? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Absence of accountable entity in the EU					X	

[15] Study from the European Parliament on "Cryptocurrencies and Blockchain", July 2018

Exchanges should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					X	
Exchanges should segregate the assets of users from those held on own account					X	
Exchanges should be subject to rules on conflicts of interest				X		
Exchanges should be required to keep appropriate records of users' transactions					X	
Exchanges should have an adequate complaints handling and redress procedures				X		
Exchanges should be subject to prudential requirements (including capital requirements)	X					
Exchanges should be subject to advertising rules to avoid misleading marketing/promotions					X	
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)					X	
Exchanges should be responsible for screening crypto-assets against the risk of fraud					X	
Other					X	

Please indicate if those requirements should be different depending on the type of crypto-assets available on the exchange and explain your reasoning (if needed).

An important measure against money laundering and financing of terrorism is for an exchange to know their customers. Therefore, it should be implemented whenever the nature of the crypto-asset creates exposure to that risk. See also our answer to question 29.

4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys[16] 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[17]. 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.

[16] 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.

[17] 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.

31) In your opinion, what are the main risks in relation to the custodial wallet service provision? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
No physical presence in the EU					X	
Lack of adequate governance arrangements, including operational resilience and ICT security					X	
Absence or inadequate segregation of assets held on the behalf of clients					X	
Conflicts of interest arising from other activities (trading, exchange)			X			
Absence/inadequate recordkeeping of holdings and transactions made on behalf of users					X	
Absence/inadequate complaints or redress procedures are in place			X			
Bankruptcy of the custodial wallet provider					X	
Inadequate own funds to repay the consumers				X		
Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)					X	
The custodial wallet is compromised or fails to provide expected functionality				X		
The custodial wallet provider behaves negligently or fraudulently				X		
No contractual binding terms and provisions with the user who holds the wallet				X		
Other						

Please explain your reasoning (if needed).

The risks depend on the different business models of custodial wallet providers, and the specific type of assets that they safeguard. Those wallet providers that keep all customers' assets into one "master wallet" are more open to prudential risks than those that merely register customers' private keys (so that the funds of an individual customer is held on a specific individual address).

Something that is missing in the table above, are ML and TF risks. Custodial wallet providers have become gatekeepers to the financial system with the introduction of AMLD5. Therefore, these parties have a responsibility with regards to AML and CFT. Wallets can be used to perform transactions or hide funds in a matter that is not compliant with AML, CFT or criminal law. This is especially the case when a custodial wallet allows the storage of so-called privacy coins (or anonymity enchacing coins).

32) What are the requirements that could be imposed on custodial wallet providers in order to mitigate those risks? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Custodial wallet providers should have a physical presence in the EU					X	

Custodial wallet providers should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					X	
Custodial wallet providers should segregate the asset of users from those held on own account					X	
Custodial wallet providers should be subject to rules on conflicts of interest					X	
Custodial wallet providers should be required to keep appropriate records of users' holdings and transactions					X	
Custodial wallet providers should have an adequate complaints handling and redress procedures					X	
Custodial wallet providers should be subject to capital requirements				x		
Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions					X	
Custodial wallet providers should be subject to certain minimum conditions for their contractual relationship with the consumers/investors					X	
Other						

Please indicate if those requirements should be different depending on the type of crypto-assets kept in custody by the custodial wallet provider and explain your reasoning (if needed).

Depending on the type of crypto asset that a wallet can safeguard, specific requirements can be explored. Safeguarding security and transaction tokens probably involve other risks than safeguarding utility tokens or other digital assets.

A general measure worth considering is to require custodial wallet providers to have mitigation plans in place to hand back ownership of a private key to the customer, and to a different custodial wallet provider in case of a (looming) bankruptcy. Furthermore, independent of specific business model, regulation on mitigating operational and cyber risks could be considered.

Regarding AML/CFT, the regulations stemming from AMLD5 should be expanded upon so that the recently adopted FATF-standards on virtual assets are adopted on the EU-level. In case of custodial wallets, it at least means that they will need to adhere to the so-called travel rule. However, the travel rule should only be introduced when a workable solution available.

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**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

This should be possible, but only if sufficient requirements are in place, if the wallet is MiFID II compliant and if the wallet is properly supervised. Again, proportionality and functionality must be kept in mind. The specific functionalities of the crypto assets that a wallet safeguards determines the specific requirements they should adhere to. If a crypto assets qualify under MiFID II, it should be treated as such. It should not lead to situations where a specific wallet is exempted from MiFID II, only because they are a custodial wallet.

34) In your opinion, are there certain business models or activities/services in relation to digital wallets (beyond custodial wallet providers) that should be in the regulated space?

This depends on several risk factors that these business models or activities/services might produce, including (but not limited to) the risks that they pose to the system of AML/CFT requirements, prudential risks that they pose to other financial institutions, and possibilities of regulatory arbitrage with products that are otherwise regulated. However, any regulation on these models beyond custodial wallet providers should be technically feasible and proportional, and should not be an impediment to innovation or small business growth. Furthermore, financial regulation can only be applied to obliged entities, and not to individual citizens.

5. Other service 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.

35) In your view, what are the services related to crypto-assets that should be subject to requirements? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant"[18].

	1	2	3	4	5	No opinion
Reception and transmission of orders in relation to crypto-assets					X	
Execution of orders on crypto-assets on behalf of clients					X	
Crypto-assets portfolio management					X	
Advice on the acquisition of crypto-assets					X	
Underwriting of crypto-assets on a firm commitment basis					X	
Placing crypto-assets on a firm commitment basis				X		

[18] 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.

Placing crypto-assets without a firm commitment basis				X		
Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)					X	
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)					X	
Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)					X	
Services provided by developers that are responsible for maintaining/updating the underlying protocol					X	
Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)					X	
Other services						

Please illustrate your response, by underlining the potential risks raised by these services if they were left unregulated and by identifying potential requirements for those service providers.

We have filled out the table with the limited focus on those crypto assets that qualify as an investment token. As mentioned before, investment tokens should be regulated similarly to traditional financial instruments as the risks of the instruments themselves have not changed. For other types of tokens we consider the need for regulation on the basis of the abovementioned services less relevant or proportionate.

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)[19], 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.

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?**

- **Yes**
- **No**
- **Partially**
- **Don't know/no opinion**

[19] Payment Services Directive 2 (2015/2366/EU)

Please explain your reasoning (if needed).

PSD2 has been designed with the intention to create a level playing field among payment services providers and to set the common ground rules for those professional parties operating within the payments space. As mentioned, crypto assets are not covered by PSD2 (unless it specifically qualifies as e-money) as they do not qualify as funds. In our view transaction tokens are different from bank money, cash and (generally) e-money.

Furthermore, PSD2 has not been designed taking crypto assets and crypto asset service providers in mind. A custodial wallet is (generally) different from a regular bank account or e-money account, for example. A situation where crypto assets (and service providers) are "pushed" into the PSD2 regime may be ineffective and could create unwanted legal loopholes. Therefore, it would be unwise to, from the outset, place transaction tokens under the PSD2 regime. This would also contribute to a fair and proportionate legal framework for crypto assets.

That said, there might be some provisions in PSD2 that might be used (or adapted) to regulate specific crypto asset activities or operations that are similar to the regulated entities under PSD2. This would of course depend on the functionalities of transaction tokens. A deeper dive into the possible overlap of characteristics might therefore be desirable.

Lastly, we would like to stress that those crypto asset service proivders that do offer payment services (qualifying under PSD2), or, for example, a payment services provider that uses blockchain or DLT as the backbone of its operations to provide payment services (qualifying under PSD2), should be regulated under PSD2.

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.

37) In your opinion, what are the biggest market integrity risks related to the trading of crypto-assets? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Price manipulation					X	
Volume manipulation (wash trades…)					X	

Pump and dump schemes					X	
Manipulation on basis of quoting and cancellations					X	
Dissemination of misleading information by the crypto-asset issuer or any other market participants					X	
Insider dealings					X	
Other					X	Inadequate asset segregation and custodian fraud

Please explain your reasoning (if needed).

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.

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

By introducing transparency requirements, the regulatory framework on market integrity should be applicable on crypto asset markets.

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

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed). If yes, please explain how you would see this best achieved in practice.

See the answer to question 38

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?

N/A

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[20], 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"*[21]. 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.

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**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

Yes, we consider it appropriate to extend the definition in the EU AML/CFT legal framework. Developments in this area are ongoing. Tokenisation will result in a wide variety of assets that represent value. This might change our current view on how to conduct a payment and it might open up new ways for money laundering and terrorist financing.

We are in favour of a broad legal definition of crypto-assets, which include all crypto initiatives on the market including potential new initiatives (which will be available in the future). If a narrow definition will be chosen, certain types if crypto assets will not be covered by the legal definition and these assets will not fall within the regulatory framework. This can lead to too narrow existing regulation or supervision arbitrage as parties can construct crypto-assets in a way in which it will not be covered by the legal definition. Therefore we are in favour of the broad definition of crypto assets, at least capturing the FATF definition. However, this does not necessarily means that we should simply copy the FATF definition, as it is not perfect and leaves much room for interpretation.

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

[20] Anti-Money Laundering Directive (Directive 2015/849/EU) as amended by AMLD5 (Directive 2018/843/EU)
[21] FATF Recommendations

between private persons not acting as a business, in particular when done through wallets that are not hosted by custodial wallet providers.

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? If any, please describe the possible risks to tackle.**

In this regard we follow the same line as the FATF and we are of the opinion that the following crypto-asset service providers should be added to the EU AML/CFT legal framework:
i) exchange between virtual assets and fiat currencies;
ii) exchange between one or more forms of virtual assets;
iii) transfer of virtual assets;
iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Some of these activities will already (partially) be regulated under AMLD5. However, AMLD5 does not cover all the FATF activities. As AMLD5 has already created a solid foundation for a harmonized AML/CFT framework for certain crypto asset activities, it would be very preferable to scope in all of the parties on the EU-level, rather than to rely on each member state to regulate it on the national level.

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**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

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?**

We have to look at the risks that might appear from peer-to-peer transactions internationally and in cooperation with European and global authorities. Currently, there is not a common view on the (potential) risks and the mitigation of those risks.
Before drafting new regulation, one should have a clear idea on the risks and the mitigation of those risks. Otherwise, it will be hard to create an effective regulatory framework.

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."[22]

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

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

Our preference is that implementation will be performed in a harmonised way at the EU level, analogous to how the travel rule is legislated for regular bank transfers (with the Wire transfer regulation 2 (regulation (EU) 2015/847)). In implementing the travel rule, it's important that crypto companies have the opportunity to come up with a solution themselves and not restrict them too much by adding details on practical implementation.

The travel rule should only be implemented after VASPs have had sufficient time to comply with the requirements and only when a viable solution has become available. We suggest that we look for innovative ways to obtain this info without compromising privacy and make sure that the majority of transactions are covered.

We recognize international concerns regarding technical difficulties that VASPs have to comply with these new rules. We support the initiatives at FATF level to look for different solutions that are being developed. And we recommend the EC to closely monitor those initiatives and to take them into account regarding the timing of the implementation.

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? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
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					X	
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					X	

[22] FATF Recommendations

Please explain your reasoning (if needed).

In our view, the abovementioned requirements are already necessary in order to properly implement AMLD5 into national law, as AMLD5 requires member states to be able to continuously supervise the obliged entities under AMLD5 in an effective manner. Therefore, we assume that the abovementioned requirements are already in place.

3. Consumer/investor protection[23]

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[24]. 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.

47) What type of consumer protection measures could be taken as regards crypto-assets? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Information provided by the issuer of crypto-assets (the so-called 'white papers')					X	
Limits on the investable amounts in crypto-assets by EU consumers			X			
Suitability checks by the crypto-asset service providers (including exchanges, wallet providers…)					X	
Warnings on the risks by the crypto-asset service providers (including exchanges, platforms, custodial wallet providers…)					X	
Other						

Please explain your reasoning and indicate if those requirements should apply to all types of crypto assets or only to some of them.

[23] 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.

[24] ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019

Depending on the type of asset different measures should apply. Looking at investment crypto's or tokens, similar rules should apply as for financial instruments.

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?

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

Yes, because these assets / tokens have different functions and give clients different types of rights, rules should relate to that.

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'*)[25].

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?

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

Yes, because this would be in accordance with the current system.

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)?

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain your reasoning (if needed).

[25] See Autorité des Marchés Financiers, French ICOs – A New Method of financing, November 2018

The type of asset is of essential importance. Investment cryptos, should be considered as financial instruments and the relevant regulatory regime should apply accordingly.

The vast majority of crypto-assets that are accessible to EU consumers and investors are currently issued outside the EU[26]. 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.

51) In your opinion, how should the crypto-assets issued in third countries and that would not comply with EU requirements be treated? Please rate each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".

	1	2	3	4	5	No opinion
Those crypto-assets should be banned			X			
Those crypto-assets should be still accessible to EU consumers/investors					X	
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					X	
Other						

Please explain your reasoning (if needed).

Crypto assets issued in third countries which do not meet the EU requirements should be prohibited in the EU, if these assets are issued in third countries where there is no equivalent regulatory regime.

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[27]. 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

[26] In 2018, for instance, only 10% of the crypto-assets were issued in the EU (mainly, UK, Estonia and Lithuania) – Source: Satis Research.

[27] https://www.ecb.europa.eu/paym/pol/html/index.en.html

their global reach 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.

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 (if needed).

EU coordination is highly desirable in order to assure level-playing-field and avoid regulatory arbitrage. It is also necessary to have a level playing field for financial service providers - including crypto asset service providers - across Europe. Given the cross-border nature of crypto assets, supervisory coordination among member states is desirable. Certain regulatory measures, such as the AML/CTF measures, are implemented on a national level by member states.

Global risks, such as transmission of monetary policy and liquidity risks concern the European financial system as a whole. The cross-border payment infrastructure should therefore, where possible, be regulated by European Authorities, using a harmonised regulatory framework. The regulatory framework should include requirements to deal with the specificities of the technology, for instance global stablecoins. Furthermore, AML/CFT supervision on crypto assets, precisely because of their cross-border nature, would be more efficient and effective on EU-level (which The Netherlands advocates more generally as well).

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

EU regulators would benefit from a harmonised regulatory regime on crypto assets that is applicable to a changing and innovating sector. Currently, is not always clear how to apply both national and international regulations to new initiatives. A European regulatory framework and a harmonized approach on EU level would benefit both the sector and the regulators.
Furthermore, it is still a big fundamental question whether regulators / supervisors should even look (closely) at the underlying technologies. Currently, financial supervisors don't supervise IT-systems.

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[28] 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[29], 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[30] 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)[31] 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.

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[32], with none of them having been admitted to trading or traded on a trading venue nor admitted in a CSD book-entry system[33].

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[34]. Such activities would be overseen by a central body or operator, *de facto* similarly to traditional

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

[29] European Markets Infrastructure Regulation (648/2012/EU)

[30] ESMA, 'Advice on Initial Coin Offerings and Crypto-Assets', January 2019

[31] 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.

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

[33] See section IV.2.5 for further information

[34] 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.

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[35] 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[36] 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.

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)?]

Please refer to this website for an overview of STOs. It seems to be quite accurate.

https://stoscope.com/stos?sort=&status=all&category=all&asset_class=all&token_right=all&country=162&profile=20

[35] 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.

[36] 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.

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	
Rather agree	X
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed). If you agree, please indicate the specific areas where, in your opinion, the technology could afford most efficiencies when compared to the legacy system.

At its core, DLT is an IT-solution, and has pro's and con's much like any other IT-solution. The requirements for the use of IT-systems in the financial sector are technology neutral.

DLT innovates those business model where, traditionally, a trusted third party is needed. All parties involved can all use the exact same ledger on which ownership is recorded, therefore bypassing all inefficiencies that are inherent to the traditional models. Examples are trading, post-trade and asset management, such as found with payment service providers and CCPs. On the other hand however, it seems that, at this moment, current DLTs are unable to process large quantities of transactions. Nonetheless, we see the potential that DLT can bring to some of the "backbone" technologies of these service, and that it can be a potential contribution to the financial services industry.

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?

Completely agree	
Rather agree	
Neutral	X
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed).

As mentioned before, DLT is a technology with pro's and con's. It furthermore depends on the type of DLT that is used in a specific business model, as well as how it interacts with the other core activities of the business. Further research into the potential stability risks of this technology of trading and post-trade services is needed.

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.

In a traditional transaction of a financial instrument, seven or more parties are involved (from order submission to settlement). DLT could be used in order to make the division of these roles less fragmented.

Trading venues would probably still play a role, as they are needed for the operation of the platform and trading, for enforcing trading rules and a the central party for distribution of information on the traded assets. Depending on the ability of the used DLT to settle transactions real-time and immediately, and therefore reducing counterparty risks, CCPs could be impacted. Lastly, CSDs could potentially lose their booking function, as transactions would be recorded in the distributed ledger. However, their function as a custodian of safe keeper of assets will probably remains needed.

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?

Completely agree	
Rather agree	X
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed).

Apparently, current regulations are unclear to the market. This is something that has been flagged on a national level as well. Therefore, it would be interesting to give more guidance of clarification of the how the current regulation applies (where possible). Care should be taken, however, to distinguish between using DLT in the core systems of regulated entities on one hand, and trading security tokens as an asset on the other. These are two different issues and concepts. However, it is also the responsibility of market participants to understand their own products and business operations, and do due (legal) diligence before starting operations.

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)[37] and a regulation (MiFIR)[38] and their delegated and implementing 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[39] 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.

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	
Rather agree	X
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

[37] Market in Financial Instruments Directive (2014/65/EU)
[38] Markets in Financial Instruments Regulation (600/2014/EU)
[39] ESMA, 'Advice on Initial Coin Offerings and Crypto-Assets', January 2019

Please explain your reasoning (if needed).

60) **If you consider that this is an impediment, what would be the best remedies according to you? Please rate each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".**

	1	2	3	4	5	No opinion
Harmonise the definition of certain types of financial instruments in the EU					X	
Provide a definition of a security token at EU level					X	
Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token					X	
Other						

Please explain your reasoning (if needed).

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)? Please rate each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".**

	1	2	3	4	5	No opinion
Hybrid tokens should qualify as financial instruments/security tokens					X	
Hybrid tokens should qualify as unregulated crypto-assets (i.e. like those considered in section III. of the public consultation document)	X					
The assessment should be done on a case-by-case basis (with guidance at EU level)					X	
Other						

Please explain your reasoning (if needed).

As explained before, hybrid tokens as such should not be identified as an independent type of token, and a case-by-case approach should be taken (see answer to question 8). If a token qualifies both as a transaction and investment token, it should be regulated as both. Regarding the table above, a hybrid token should only qualify as an investment token as it qualifies as such.

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.

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

Completely agree	X
Rather agree	
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed).

Because they provide the same function as what is currently regulated (level-playing-field / tech agnostic). Plus the risks associated with these offerings are quite similar.

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

Completely appropriate	X
Rather appropriate	
Neutral	
Rather appropriate	
Completely inappropriate	
Don't know / No opinion	

Please explain your reasoning (if needed).

There seems to be demand from the sector for more clarification. Therefore, clarification in the form of guidance could be a possibility.

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.

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

Completely appropriate	X
Rather appropriate	
Neutral	

Rather inappropriate	
Completely inappropriate	
Don't know / No opinion	

Please explain your reasoning (if needed).

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 (if needed).

In principle the answer is no, but the regime is a barrier in itself as it contains a lot of rules. It is considered very heavy by startups.

Please explain your reasoning (if needed).

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[40], 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[41].

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 (if needed).

It depends on the type of DLT used by the trading venue. Current legislation (art 48 MiFID II / RTS7) requires trading venues to have in place outsourcing arrangements

[40] ESMA, 'Advice on Initial Coin Offerings and Crypto-Assets', January 2019

[41] Recital 8 of MiFIR.

including control mechanisms for critical functions (which DLT could considered to be). If a trading venue want to use an open public DLT, this could be an issue.

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.

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 (if needed).

We believe that the current regulation is appropriate.

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 (if needed).

The current legislation is appropriate, but inherent risks of investing in security tokens should be disclosed in a transparent and understandable manner.

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

No, MiFiD already applies for security tokens. If a token is not regulated under MiFiD a special crypto framework would be most welcome. We do not favour a change in the existing MiFID/MiFIR requirements.

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.

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 (if needed).

Yes it could as the technology makes it easier and more efficient to issue and trade tokens. So it could work in markets that are not in need of liquidity / multilateral margining etc.

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[42] 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.

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

See our answer to question 27. For extra literature, see the new paper of IOSCO (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf).

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.

[42] 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)

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

No

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.

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

MiFID does not limit access to trading venues of any type of participant but requires of any type of participant to fulfil the appropriate requirements in order to ensure the proper functioning of the financial markets. The biggest hurdles are the abovementioned requirements b) and d). Depending on the transposition in national legislation, it is not always possible for trading venues to protect the client sufficiently when dealing with complex instruments. So, the proper protection of retail clients prevents direct access of retail clients, not the proper functioning of the markets. Another legal challenge is the “No LEI, no trade” aspect of MiFID, but identification of UBO could easily be fixed by the trading venue, by means of membership admission criteria. The requirement to have sufficient resources can be met by retail in systems which operate real time settlement processes that pre-check availability of cash and instruments. Clearing is not required and financial risks to the system can be adequately mitigated.

1.10. Pre and post-transparency requirements

MiFIR[43] 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

[43] In its Articles 3 to 11

tokens. The availability of data could perhaps be an issue for best execution[44] 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.

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

Completely agree	
Rather agree	X
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed).

Yes, because it is a financial instrument. Please refer to the guiding principles for the post-trade processing of tokenized securities.

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 (if needed).

This depends on the type of trading of security tokens. For instance, with trading whereby orders are immediately matched and transactions are executed, a more flexible approach towards pre-trade transparency could be beneficial. If using an order book and delayed execution of orders, pre-trade transparency remains needed.

In both scenarios post trade transparency remains pivotal to the price discovery process.

1.11. Transaction reporting and obligations to maintain records

MiFIR[45] 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).

[44] 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.

[45] In its Article 25 and 26

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

Please refer to the guiding principles for the post-trade processing of tokenized securities.

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[46] 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.

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?

Inside information must relate to one or more issuers of financial instruments or to one or more financial instruments. In case these financial instruments (security tokens) are traded on a trading venue or the price or value depends on such financial instrument, they should be covered by MAR.

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.

[46] Under MiFID Article 4(1)(24) 'trading venue' means a regulated market (RM), a Multilateral Trading Facility (MTF) or an Organised Trading Facility (OTF')

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.

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?

Provided that these financial instruments (security tokens) are traded on a MiFID II trading venue or the price or value depends on such financial instrument (e.g. Article 2 MAR) the difference in transacting and security tokens should be covered at least by 'any other behaviour' (a) or 'any other activity' (b).

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?

There could be additional issues and risks related to the technology used. Depending on how blockchain is used, the type of blockchain (permissioned vs. permissionless) type of consensus mechanism etc. conflicts of interests could arise, prices can be manipulated etc.

3. Short Selling Regulation (SSR)

The Short Selling Regulation[47] (SSR) sets down rules that aim to achieve the following objectives: (i) increase transparency of significant net short positions held by investors; (ii) reduce settlement risks and other risks associated with uncovered short sales; (iii) reduce risks to the stability of sovereign debt markets by providing for the temporary suspension of short-selling activities, including taking short positions via sovereign credit default swaps (CDSs), where sovereign debt markets are not functioning properly. The SSR applies to MiFID II financial instruments admitted to trading on a trading venue in the EU, sovereign debt instruments, and derivatives that relate to both categories.

According to ESMA's advice[48], security tokens fall in the scope of the SSR where a position in the security token would confer a financial advantage in the event of a decrease in the price or value of a share or sovereign debt. However, ESMA remarks that the determination of net short positions for the application of the SSR is dependent on the list of financial instruments set out in Annex I of Commission Delegated Regulation (EU) 918/2012), which should therefore be revised to include those security tokens that might generate a net short position on a share or on a sovereign debt. According to ESMA, it is an open question whether a transaction in an unregulated crypto-asset could confer a financial advantage in the event of

[47] Short Selling Regulation (236/2012/EU)

[48] ESMA, 'Advice on Initial Coin Offerings and Crypto-Assets', January 2019

a decrease in the price or value of a share or sovereign debt, and consequently, whether the Short Selling Regulation should be amended in this respect.

80) Have you detected any issues that would prevent effectively applying SSR to security tokens? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
transparency for significant net short positions						X
restrictions on uncovered short selling						X
competent authorities' power to apply temporary restrictions to short selling						X
Other						

Please explain your reasoning (if needed).

Provided these financial instruments (security tokens) fall within the scope Article 1 SSR, (are admitted to trading on an EU trading venue, or that relate to such instruments or issuer, or mentioned debt instruments) there should not be an issue.

81) Have you ever detected any unregulated crypto-assets that could confer a financial advantage in the event of a decrease in the price or value of a share or sovereign debt?

N.A. / We do not know, because currently no security tokens are admitted to trading on a Dutch RM / MTF / OTF.

4. Prospectus Regulation (PR)

The Prospectus Regulation[49] 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

[49] Prospectus Regulation (2017/1129/EU)

offers to the public under Article 1(4) or for admission to trading on a RM under Article 1(5) applies.

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 agree	
Rather agree	
Neutral	
Rather disagree	X
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed).

We do not have any experience yet in securitizing STO prospectuses. However, we do think that different and/or exemptions should apply to security tokens additional to the exemptions of Article 1 (4) and article 1 (5) PR. Different and/or additional exemptions are necessary for this type of securities because of the typical characteristics. However, additional exemptions for security tokens could result in issuers only issuing security tokens (instead of regular securities) to the public in order to be exempted from the prospectus regulation. Therefore, any possible exemption should have a good purpose and must be very clear.

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[50] 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.

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

- **Yes**
- **No**
- **Don't know/no opinion**

If yes, please indicate the most effective approach: a 'building block approach' (i.e. additional information about the issuer and/or security tokens to be added as a complement to existing schedules) or a 'full prospectus approach' (i.e. completely new prospectus schedules for security tokens). Please explain your reasoning (if needed).

We think that the most effective approach would be a 'full prospectus approach' with a completely new prospectus schedule for security tokens. Probably by including references to other relevant items of 'existing' schedules to cover the minimum prospectus information disclosure.

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

We do not have any experience with this so far**.**

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 (if needed).

We do not have any experience with this so far.

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?

- **Yes**
- **No**

[50] ESMA, Guidelines on Risks factors under the prospectus regulation (31-62-1293)

- **Don't know/no opinion**

Please explain your reasoning (if needed).

If it is to stimulate the provision of security tokens within Europe, then we could understand why an alleviated prospectus type or regime is useful.

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

Completely agree	X
Rather agree	
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

If you agree, please indicate if ESMA's guidelines on risks factors should be amended accordingly. Please explain your reasoning (if needed).

The principles of the ESMA's guidelines on risk factors can also be applied to the issuance of investment tokens.

5. Central Securities Depositories Regulation (CSDR)

CSDR[51] 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

[51] Central Securities Depositories Regulation (909/2014/EU)

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.

88) Would you see any particular issue (legal, operational, technical) with applying the following definitions in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern"

	1	2	3	4	5	No opinion
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		X				
definition of 'securities settlement system' and whether a DLT platform can be qualified as securities settlement system under the SFD		X				
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;		X				
definition of 'book-entry form' and 'dematerialised form	X					
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);		X				
what could constitute delivery versus payment in a DLT network, considering that the cash leg is not processed in the network		X				
what entity could qualify as a settlement internaliser		X				
Other						

Please explain your reasoning.

The legal issue is that ownership and the transfer of the security token is recorded in the DLT, which is not necessarily identical to the books of a CSD (which is the requirement). Other issues are currently not foreseen as CSDR is technology neutral and therefore DLT could fit into the existing legislation. While DvP is the ultimate goal, settlement of the cash leg in central bank money today is also not in the current IT-infrastructure of the CSD.

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

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain your reasoning.

Most CSDs today already process digital representation of securities. Security tokens are digital representations of the underlying security, this should be no issue in terms of CSDR book-entry requirements.

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.

Dutch legislation does not prevent the use of DLT.

91) Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system	X					
Rules on measures to prevent settlement fails	X					
Organisational requirements for CSDs	X					
Rules on outsourcing of services or activities to a third party	X					
Rules on communication procedures with market participants and other market infrastructures	X					
Rules on the protection of securities of participants and those of their clients	X					
Rules regarding the integrity of the issue and appropriate reconciliation measures	X					
Rules on cash settlement	X					
Rules on requirements for participation	X					
Rules on requirements for CSD links	X					
Rules on access between CSDs and access between a CSD and another market infrastructure	X					
Other (including other provisions of CSDR, national rules applying the EU acquis, supervisory practices, interpretation, applications…)		X				

Please explain your reasoning (if needed).

While we believe that current settlement legislation does not prevent the use of DLT, we do not have practical experiences nor evidence and our view is based on assumptions.

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[52]? Please explain your reasoning.

In the Netherlands, the Securities Giro Act (Wet giraal effectenverkeer) sets out additional requirements, for instance insolvency of a CSD, identification of UBOs etc.

6. Settlement Finality Directive (SFD)

The Settlement Finality Directive[53] lays down rules to minimise risks related to transfers and payments of financial products, especially risks linked to the insolvency of participants in a transaction. It guarantees that financial product transfer and payment orders can be final and defines the field of eligible participants. SFD applies to settlement systems duly notified as well as any participant in such a system.

The list of persons authorised to take part in a securities settlement system under SFD (credit institutions, investment firms, public authorities, CCPs, settlement agents, clearing houses, system operators) does not include natural persons. This obligation of intermediation does not seem fully compatible with the functioning of crypto-asset platforms that rely on retail investors' direct access.

93) Would you see any particular issue (legal, operational, technical) with applying the following definitions in the SFD or its transpositions into national law in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
definition of a securities settlement system						X
definition of system operator						X
definition of participant						X
definition of institution						X
definition of transfer order						X
what could constitute a settlement account						X
what could constitute collateral security						X
Other						

Please explain your reasoning.

Firstly, it is the question whether SFD is needed in business models using DLT. We think that SFD is needed to reduce the negative impact of insolvency of participants to the system. If there is netting of transactions in the DLT, the unbundling of netted transactions could require finality to protect the system. But to our knowledge, a fundamental aspect of DLT is that it is a real time gross settlement system in which SFD is necessarily needed.

[52] Such as the requirements regarding the recording on an account with a custody account keeper outside a DLT environment

[53] Settlement Finality Directive (98/26/EC)

94) SFD sets out rules on conflicts of laws. According to you, would there be a need for clarification when applying these rules in a DLT network[54]? Please explain your reasoning.

N/A

95) In your Member State, what requirements does your national law establish for those cases which are outside the scope of the SFD rules on conflicts of laws?

N/A

96) Do you consider that the effective functioning and/or use of DLT solution is limited or constrained by any of the SFD provisions?

- **Yes**
- **No**
- **Don't know/no opinion**

If yes, please provide specific examples (e.g. provisions national legislation transposing or implementing SFD, supervisory practices, interpretation, application…). Please explain your reasoning.

N/A

7. Financial Collateral Directive (FCD)

The Financial Collateral Directive[55] aims to create a clear uniform EU legal framework for the use of securities, cash and credit claims as collateral in financial transactions. Financial collateral is the property provided by a borrower to a lender to minimise the risk of financial loss to the lender if the borrower fails to meet their financial obligations to the lender. DLT can present some challenges as regards the application of FCD. For instance, collateral that is provided without title transfer, i.e. pledge or other form of security financial collateral as defined in the FCD, needs to be enforceable in a distributed ledger[56].

97) Would you see any particular issue (legal, operational, technical) with applying the following definitions in the FCD or its transpositions into national law in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

[54] In particular with regard to the question according to which criteria the location of the register or account should be determined and thus which Member State would be considered the Member State in which the register or account, where the relevant entries are made, is maintained.

[55] Financial Collateral Directive (2002/47/EC)

[56] ECB Advisory Group on market infrastructures for securities and collateral, "the potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration" (2017)

	1	2	3	4	5	No opinion
if crypto-assets qualify as assets that can be subject to financial collateral arrangements as defined in the FCD					X	
if crypto-assets qualify as book-entry securities collateral						X
if records on a DLT qualify as relevant account						X
Other						X

Please explain your reasoning.

Collateral provides security for certain financial transactions. Crypto assets are known for their volatility, so they will not provide the required safety. Furthermore, the services for collateral management are very expensive and hard to fulfil properly. With regards to relevant accounts, it is necessary to have a physical location in order to have legal certainty.

98) FCD sets out rules on conflict of laws. Would you see any particular issue with applying these rules in a DLT network[57]?

Yes, especially if there uncertainty about where the DLT network is located.

99) In your Member State, what requirements does your national law establish for those cases which are outside the scope of the FCD rules on conflicts of laws?

N/A

100) Do you consider that the effective functioning and/or use of a DLT solution is limited or constrained by any of the FCD provisions?

- **Yes**
- **No**
- **Don't know/no opinion**

If yes, please provide specific examples (e.g. provisions national legislation transposing or implementing FCD, supervisory practices, interpretation, application…). Please explain your reasoning.

8. European Markets Infrastructure Regulation (EMIR)

The European Markets Infrastructure Regulation (EMIR)[58] applies to the central clearing, reporting and risk mitigation of over-the-counter (OTC) derivatives, the clearing obligation for certain OTC derivatives, the central clearing by central counterparties (CCPs) of contracts traded on financial markets (including bonds, shares, OTC derivatives, Exchange-Traded

[57] in particular with regard to the question according to which criteria the location of the account should be determined and thus which country would be considered the country in which the register or account, where the relevant entries are made, is maintained

[58] European Markets Infrastructure Regulation (648/2012/EU)

Derivatives, repos and securities lending transactions) and services and activities of CCPs and trade repositories (TRs).

The central clearing obligation of EMIR concerns only certain OTC derivatives. MiFIR extends the clearing obligation by CCPs to regulated markets for exchange-traded derivatives. At this stage, however, the Commission services does not have knowledge of any project of securities token that could enter into those categories.

A recent development has also been the emergence of derivatives with crypto-assets as underlying.

101) Do you think that security tokens are suitable for central clearing?

Completely appropriate	X
Rather appropriate	
Neutral	
Rather inappropriate	
Completely inappropriate	
Don't know / No opinion	

Please explain your reasoning (if needed).

A security token is a digital representation of an asset. Technically there is no obvious reason why transactions in these security tokens cannot be centrally cleared.

102) Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
Rules on margin requirements, collateral requirements and requirements regarding the CCP's investment policy			X			
Rules on settlement			X			
Organisational requirements for CCPs and for TRs			X			
Rules on segregation and portability of clearing members' and clients' assets and positions			X			
Rules on requirements for participation			X			
Reporting requirements			X			
Other (including other provisions of EMIR, national rules applying the EU acquis, supervisory practices, interpretation, applications…)			X			

Please explain your reasoning (if needed).

As DLT is, in principle, an IT solution, and it can be deployed in central clearing as long as it fulfils the regulatory requirements. The latency of existing DLT systems will prevent any large scale application of DLT. Also, if the DLT is public there may be difficulties to achieve compliance with EMIR requirements.

103) Would you see the need to clarify that DLT solutions including permissioned blockchain can be used within CCPs or TRs?

No.

104) Would you see any particular issue with applying the current rules to derivatives the underlying of which are crypto assets, in particular considering their suitability for central clearing? Please explain your reasoning (if needed).

We believe that the current rules are sufficient.

9. The Alternative Investment Fund Directive

The Alternative Investment Fund Managers Directive[59] (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 'security 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.

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? Please rate each proposal from 1 to 5, 1 standing for "not suited" and 5 for "very suited".

	1	2	3	4	5	No opinion
AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;	X					
AIFMD provisions requiring AIFMs to maintain and operate effective organisational and administrative		X				

[59] Alternative Investment Fund Managers Directive (2011/61/EU)

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;	X					
AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets;	X					
Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments.	X					
Other						

Please explain your reasoning (if needed).

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?

- **Yes**
- **No**
- **Don't know/no opinion**

If yes, please provide specific examples with relevant provisions in the EU acquis. Please explain your reasoning (if needed).

In the case that an AIFM invests in securities tokens, we think it will be hard to comply with the requirements of the AIFMD, such as but not limited to: the appointment of a depositary, valuation, risk management, liquidity management and certain reporting requirements. DLT could however support e.g. the administration of fund documents and the administration of participants.

10. The Undertakings for Collective Investment in Transferable Securities Directive (UCITS Directive)

The UCITS Directive[60] applies to UCITS established within the territories of the Member States and lays down the rules, scope and conditions for the operation of UCITS and the authorisation of UCITS management companies. The UCITS directive might be perceived as potentially creating challenges when the assets are in the form of 'security tokens', relying on DLT.

For instance, under the UCITS Directive, an investment company and a management company (for each of the common funds that it manages) shall ensure that a single depositary is appointed. The assets of the UCITS shall be entrusted to the depositary for safekeeping. For crypto-assets that are not 'security tokens' (those which do not qualify as financial

[60] Undertaking for Collective Investment in Transferable Securities Directive (2009/65/EC)

instruments), the rules for 'other assets' apply under the UCITS Directive. 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. This function could arguably cause perceived uncertainty where such assets are security tokens.

107) Do the provisions of the EU UCITS Directive legal framework in the following areas are appropriately suited for the effective functioning of DLT solutions and the use of security tokens? Please rate each proposal from 1 to 5, 1 standing for "not suited" and 5 for "very suited".

	1	2	3	4	5	No opinion
Provisions of the UCITS Directive pertaining to the eligibility of assets, including cases where such provisions are applied in conjunction with the notion "financial instrument" and/or "transferable security"	X					
Rules set out in the UCITS Directive pertaining to the valuation of assets and the rules for calculating the sale or issue price and the repurchase or redemption price of the units of a UCITS, including where such rules are laid down in the applicable national law, in the fund rules or in the instruments of incorporation of the investment company;	X					
UCITS Directive rules on the arrangements for the identification, management and monitoring of the conflicts of interest, including between the management company and its clients, between two of its clients, between one of its clients and a UCITS, or between two -UCITS;			X			
UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;	X					
Disclosure and reporting requirements set out in the UCITS Directive.				X		
Other						

Please explain your reasoning (if needed).

These answer were given on the basis that the UCITS directive has very stringent rules on all these matters. And the current crypto markets or tokens are not able to fulfil all these requirements (for example because of the extremely high volatility and limited liquidity.

11. Other final comments and questions as regards security 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.

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**
- **No**
- **Don't know/no opinion**

If yes, please explain the regulatory approach that you favour. Please explain your reasoning (if needed).

We describe a permissionless blockchain as a ledger in which everyone can join the user network without providing a real identity. The fact that identification is an indispensable step within financial services means that issues surrounding completely permissionless blockchains are irrelevant, since identification is necessary. It is important to note that a hybrid form would be possible, namely a public blockchain as an infrastructure (think of Ethereum) with a permissioned environment on it. You can state that the concept of a completely permissionless ledger does not coincide with conventional achievements such as the rule of law, as enshrined in legislation and regulations. Including all sorts of rules on rights, obligations and in which responsibilities are invested, depending on the type of jurisdiction.

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

Background

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.

Although DLT was welcomed by many as a revolution in clearing and settlement of securities, because real-time settlement is considered possible (T + 0), in practice T + 2 will remain the standard. At first glance, immediate settlement of a transaction seems to have advantages. For example, it is not necessary to deposit a reserve to secure the transaction against non-payment or non-delivery. In this scenario, settlement failure is theoretically and practically impossible. But this argument completely ignores the role of credit extension that has come to embody the settlement process. This function is essential for the functioning of the securities markets from a liquidity perspective.

- For more information, please read: K. Monahan: '*Steampunk Settlement: deploying futuristic technology to achieve an anachronistic result'* (Q2 2019), Greenwich.

Technological limitations: blockchain trilemma
A powerful way to look at the limitations is through the lens of Vitalik Buterin's blockchain trilemma. The starting point for this is that you can only optimize a blockchain on two of the following three essential factors. These concern: decentralization, scalability and security. In other words, all three cannot be maximized in one go and increasing the level of one factor results in the decrease of another. That is why the goal of striving for maximum levels of decentralization inherently leads to a decrease in scalability and / or security. As security within the financial sector cannot be compromised and scalability is a prerequisite for creating a liquid market and a sufficient number of transactions per second, current DLT applications often make up for the decentralized nature of the blockchain. A common misconception is that central versus decentralized is a binary concept, in practice various variations are possible.

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?

- **Yes**
- **No**
- **Don't know/no opinion**

If yes, please identify the issues that should be addressed at EU level and the approach to address them. Please explain your reasoning (if needed).

No not necessarily. Different components of blockchain technology could be used in these processes. The separation of trading and post-trading activities serve several economic and legal purposes (as explained in previous answers, not just this section but our answer provided under question 27 is also relevant).

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?

- **Yes**
- **No**
- **Don't know/no opinion**

Please provide specific examples and explain your reasoning (if needed).

We do not allow purely decentralized and fully permissioned ledgers.

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**
- **No**
- **Don't know/no opinion**

Please provide specific examples (national provisions, implementation of EU acquis, supervisory practice, interpretation, application…). Please explain your reasoning (if needed).

See our previous answers about this matter.

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)[61] sets out the rules for the business practices and supervision of e-money institutions.

In its advice on crypto-assets[62], 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[63] (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.

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

- **Yes**

[61] Electronic Money Directive (2009/110/EC)
[62] EBA report with advice for the European Commission on "crypto-assets", January 2019
[63] Payment Services Directive 2 (2015/2366/EU)

- **No**
- **Don't know/no opinion**

Please provide specific examples (EMD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application…). Please explain your reasoning (if needed).

The EMD2's requirements on initial capital and ongoing funds, safeguarding requirements, issuance, redeemability, use of agents and out of court complaint and redress procedures could also be appropriate for stablecoins. However, an e-money token (e.g. stablecoin) could have the intention (or potential) to become of systemically importance (impacting the real economy by becoming a widely used means of payment, a store of value and/ or used widely as substitute for domestic currency). We note that EMD2 was not specifically designed to regulate systematically important 'e-money tokens' (e.g. global stablecoins). Therefore, EMD2 does not seem to deal explicitly with financial stability risks, monetary sovereignty/monetary policy transmission.

A novel regime which does deal with these issues not only mitigates the risks to financial stability and monetary policy transmission, but also creates a level playing field for potential global stablecoins and other crypto-assets in the financial industry. When stablecoins are forced under EMD2 regulation supervision would not be as effective, and at the same time not welcoming of innovation. Furthermore, it could potentially lead to regulatory arbitrage issues or that specific risks are not regulated properly.

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?

- **Yes**
- **No**
- **Don't know/no opinion**

Please provide specific examples (PSD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application…). Please explain your reasoning (if needed).

See our answer with regard to question 113. This also applies for PSD2. In fact, research carried out by DNB has concluded that the whole set of regulatory provisions available in the EU has only a limited grasp on the ecosystem of financial institutions.

In this research, DNB has analysed regulatory provisions on several domains, such as integrity, operational risks, payment infrastructure, financial stability, resolution and monetary policy. When stated in this order, we have observed decreasing adequacy of the corresponding provisions for these domains when applied to VASPs, PSPs, AIFs and EMIs. Thus, where integrity risks seem adequately addressed by current provisions, there are almost no provisions regarding financial stability and monetary policy.

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**
- **No**
- **Don't know/no opinion**

Please provide specific examples and explain your reasoning (if needed).

See our answer with regard to question 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 stablecoins") 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 stablecoin" arrangements that could pose systemic risks.

116) Do you think the requirements under EMD2 would be appropriate for "global stablecoins" (i.e. those that reach global reach) qualifying as e-money tokens? Please rate each proposal from 1 to 5, 1 standing for "completely inappropriate" and 5 for "completely appropriate").

	1	2	3	4	5	No opinion
Initial capital and ongoing funds		X				
Safeguarding requirements		X				
Issuance		X				
Redeemability		X				
Use of agents		X				
Out of court complaint and redress procedures		X				
Other						

Please explain your reasoning (if needed).

See our answer with regard to question 113.

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)?

Completely appropriate	
Rather appropriate	
Neutral	
Rather inappropriate	X
Completely inappropriate	
Don't know / No opinion	

Please explain your reasoning (if needed).

See our answer with regard to question 114.

*

* *

Abbreviations

AIF – Alternative Investment Fund

AIFM – Alternative Investment Fund Manager

AIFMD – Alternative Investment Fund Managers Directive (2011/61/EU)

AML/CFT – Anti-Money Laundering/ Combatting the Financing of Terrorism

AMLD5 – 5th Anti-Money Laundering Directive (Directive 2018/843/EU)

BCBS – Basel Committee on Banking Supervision

CCP – Central Clearing Counterparty

CDS – Credit Default Swap

CSD – Central Securities Depositories

CSDR – Central Securities Depositories Regulation (909/2014/EU)

DGSD – Deposit Guarantee Schemes Directive (2014/49/EU)

DLT – Distributed Ledger Technology

DMD – Distance Marketing of Consumer Financial Services Directive (2002/65/EC)

EBA – European Banking Authority

ECB – European Central Bank

EIOPA - European Insurance and Occupational Pensions Authority

EMD2 – Electronic Money Directive (2009/110/EC)

EMIR – European Markets Infrastructure Regulation (648/2012/EU)

ESAs – European Supervisory Authorities (EBA, EIOPA, ESMA)

ESCB – European System of Central Banks

ESMA – European Securities Market Authority

ETF– Exchange-Traded Fund

EU- European Union

FATF – Financial Action Task Force

FCD – Financial Collateral Directive (2002/47/EC)

FSB – Financial Stability Board

ICO – Initial Coin Offering

ICT – Information Communication Technologies

IPO – Initial Public Offering

ISIN – International Securities Identification Number

LEI – Legal Entity Identifier

MAR – Market Abuse Regulation (596/2014/EU)

MiFIR – Markets in Financial Instruments Regulation (600/2014/EU)

MiFID II – Markets in Financial Instruments Directive II (2014/65/EU)

MTF – Multilateral Trading Facility

NCA – National Competent Authority

OTC – Over the Counter

OTF – Organised Trading Facility

P2P – Peer-to-peer

PSD 2 – Payment Services Directive 2 (2015/2366/EU)

PR – Prospectus Regulation (2017/1129/EU)

RM – Regulated Market

SFD – Settlement Finality Directive (98/26/EC)

SME – Small Medium Enterprise

STO – Security Token Offering

SSR – Short Selling Regulation (236/2012/EU)

TR – Trade Repository

UCITS – Undertaking for Collective Investment in Transferable Securities

UCITS Directive - Undertaking for Collective Investment in Transferable Securities Directive (2009/65/EC)

VASP – Virtual Asset Service Provider (as defined by the FATF)

Definitions

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

Crypto-asset: For the purpose of the consultation, a crypto-asset is defined as a type of digital asset that may depend on cryptography and exists on a distributed ledger.

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

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

Financial instrument: those instruments specified in Section C of Annex I in MiFID II

Electronic money (e-money): '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 as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer;

E-money token: For the purpose of the consultation, e-money tokens are a type of crypto-assets that qualify as electronic money under EMD2.

Eurosystem: The Eurosystem comprises the ECB and the National Central Banks of EU Member States that have adopted the euro.

Global stablecoins: For the purpose of the consultation, a "global stablecoin" is considered as a "stablecoin" that is backed by a reserve of real assets and that can be accepted by large networks of customers and merchants and hence reach global scale.

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

Investment tokens: For the purpose of the consultation, investment tokens are a type of crypto assets with profit-rights attached to it.

Mining: a means to create new crypto-assets, often through a mathematical process by which transactions are verified and added to the distributed ledger.

Payment tokens: For the purpose of the consultation, payment tokens are a type of crypto-assets that may serve as a means of payment or exchange.

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

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

Utility tokens: For the purpose of the consultation, utility tokens are a type of crypto-assets that may enable access to a specific product or service.

Security tokens: For the purpose of the consultation, security tokens are a type of crypto-assets that qualify as a financial instruments under MiFID II.

Security token offering: an operation through which companies, entrepreneurs, developers or other promoters raise capital for their projects in exchange for 'security tokens' that they create.

Stablecoins: For the purpose of the consultation, "stablecoins" are considered as a form of payment tokens whose price is meant to remain stable through time. Those "stablecoins" are typically asset-backed by real assets or funds 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).

Trading venue: Under MiFID Article 4(1)(24), trading venue means a regulated market, a multilateral trading facility, or an organised trading facility (OTF').

Virtual Currencies: Under AMLD5, virtual currency means *'digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically'.*

Wallet provider: a firm that offers storage services to users of crypto-assets.