Brussels, 19 March 2020
FINAL

EACB response to the EC's Online Public Consultation on an EU framework for markets in crypto-assets

The **European Association of Co-operative Banks** (EACB) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.800 locally operating banks and 51,500 outlets, they serve 209 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 84 million members and 713,000 employees and have an average market share in Europe of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Questions

Highlighted in yellow the selected answer.

II. Classification of crypto-assets

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*' that could cover the digital representation of other assets (such as scriptural money).

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

Beyond the distinction 'regulated' (i.e. 'security token', 'e-money token') and unregulated crypto-assets, there may be a need for differentiating the various types of crypto-assets that currently fall outside the scope of EU legislation, as they may pose different risks. In several Member States, public authorities have published guidance on how crypto-assets should be classified. Those classifications are usually based on the crypto-asset's economic function and usually makes a distinction between 'payment tokens' that may serve as a means of exchange or payments, 'investment tokens' that may have profit-rights attached to it and 'utility tokens' that enable access to a specific product or service.

At the same time, it should be kept in mind that some 'hybrid' crypto-assets can have features that enable their use for more than one purpose and some of them have characteristics that change during the course of their lifecycle.

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

Yes
No
Don't know / no opinion / not relevant

5.1 Please explain your reasoning for your answers to question 5: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

First of all and in general, we agree with the Commission with its technologically neutral approach. Legislation should be technology agnostic / neutral whether account-based or register-based.

This said, the European Union regulates and shapes the basic legal framework. Crypto-currencies have been in discussion with companies and institutions for some time, and the EU must not make itself dependent on them. The introduction of crypto-assets appears to be purposeful in the area of conflict between central banks and commercial banks.

Question 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 / not relevant

6.1 If you think it would be useful to create a classification of crypto-assets at EU level, please indicate the best way to achieve this classification (non-legislative guidance, regulatory classification, a combination of both, ...). Please explain your reasoning: 5000 character(s) maximum including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that the best way to achieve a classification is via a non-legislative guidance on how to classify crypto-assets at EU level coming from either the ECB or the EBA and ESMA would be appreciated.

Question 7. What would be the features of such a classification? When providing your answer, please indicate the classification of crypto-assets and the definitions of each type of crypto-assets in use in your jurisdiction (if applicable) . Please explain your reasoning: 5000 character(s) maximum including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We would propose a classification based on intended functions as follows:

- Payment tokens: means of payment according to PSD2/EMD2.
- Security tokens (sometimes also called "Investment tokens"): as defined by MiFID II as "tradable securities".
- Utility tokens: Enable (discounted) access to a certain service/product/platform (like a voucher).

Concerning 'hybrid tokens', we know that they are in the market; however, we think that 'hybrid tokens' should not be considered in the classification to avoid uncertainties or grey zones, as the primary function should define the regulatory regime. Of course, we know from history that e.g. gold and cigarettes were used as means of payments or even a money market fund (according to UCITS-V) could be used as a short-term store of value similar to fiat money. Nonetheless, this does not change to intended function and the regulatory regime.

Question 8. Do you agree that any EU classification of crypto-assets should make a distinction between 'payment tokens', 'investment tokens', 'utility tokens' and 'hybrid tokens'?

Yes
No
Don't know / no opinion / not relevant

Question 8.1 If you do agree that any EU classification of crypto-assets should make a distinction between 'payment tokens', 'investment tokens', 'utility tokens' and 'hybrid tokens', please indicate if any further sub-classification would be necessary: 5000 character(s) maximum including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

See answer to Question 7. In a nutshell, we agree that any EU classification of crypto-assets should make a distinction between 'payment tokens', 'investment tokens' and 'utility tokens' based on their intended functions (the latter only for consumer protection reasons, as they are no financial instruments, but kind of "vouchers"). Concerning 'hybrid tokens', they should not be considered in the classification to avoid uncertainties or grey zones.

8.2 Please explain your reasoning for your answers to question 8: 5000 character(s) maximum including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe it would be relevant to have an EU classification of crypto-assets based on their intended functions, which makes a distinction between 'payment tokens', 'investment tokens', and 'utility tokens' in order to align the current legislation (i.e. PSD2 and MiFID II).

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

Question 9. Would you see any crypto-asset which is marketed and/or could be considered as 'deposit' within the meaning of Article 2.1(3) DGSD? 5000 character(s) maximum including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Yes, as deposit represents a claim against bank and consequently any claim represented by a crypto-asset is either deposit or e-money. Therefore the (wholesale) JP Morgan Coin and the Utility Settlement Coin would (in Europe) constitute a deposit (and fall under "E-Money").

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

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

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

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

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

	1 (not important at all)	2	3	4	5 (very important)	Don't know /no opinion /not relevant
Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs			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					

10.1 Is there any other potential benefits related to crypto-assets not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning: 5000 character(s) maximum including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a

10.2 Please explain your reasoning for your answers to question 10: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We read and understand Question 10 as meaning that the underlying technology of crypto-assets can bring benefits. Looking at the question in this way, many of the entries listed in the table can represent potential benefits but there are not necessarily real cases at the moment. For example: the only widespread coin is Bitcoin, which we think besides benefits also has the downside supporting criminal activities and speculation.

If we were to have a digital euro token, one of the biggest benefit of tokenisation could be "On-chain" Delivery vs Payment, which is understood to increase security, requires less reconciliation and less risks (counterparty, failure, …). Liquidity could also be potentially increased by giving an access to some assets to smaller investors.
One other benefit we would see is the ability for an Equity/Bond issuer or an investment manager to have access to the investor registry that is updated in real time. Finally, ICOs can be seen as an interesting alternative for in particular digital companies to raise funds, compared to current funding tools.
Concerning financial inclusion, the technology involved could bring benefits to this matter but it has also a downside aspect to consider, it can exclude those who are not digital savvy.

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. 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. 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, this might change in the future.

Question 11. In your opinion, what are the most important risks related to crypto-assets? Please rate from 1 (not important at all) to 5 (very important)

	1 (not important at all)	2	3	4	5 (very important)	Don't know /no opinion /not relevant
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					
Monetary sovereignty/monetary policy transmission						X

11.1 Is there any other important risks related to crypto-assets not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In addition to AML and CFT issues, we believe two other important risks have to be considered: Circumvention of financial sanctions and embargos and circumvention of capital controls.

11.2 Please explain your reasoning for your answers to question 11: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

What we see as major risk is the current experience of "token" used for either fraudulent and money laundering, criminal activity or factual avoidance (e.g. tax evasion).

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

Question 12. In our view, what are the benefits of 'stablecoins' and 'global stablecoins'? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Concerning stablecoins, we would like to point to the (current) uncertainty about the nature of those "stablecoins" from a legal and/or regulatory perspective: Stablecoins could – depending on the legal definition – be inter alia: (i) E-Money instrument according to EMD (issuance against deposit at the issuer and claim of the customer against the issuer); (ii) some kind of "tokenised" money market fund (with assets safeguarded at depositaries / custodians with segregated account); or (iii) a "promise for a repayment based on a system of exchanges and market-makers such as with "Libra".

Concerning 'global stablecoins', we would like to refer to what Bank of England governor Mark Carney delivered during a speech at the US Federal Reserve in August 2019. Mr Carney proposed the creation of a global digital currency as a way to stabilizing global financial systems being disturbed by trade and currency wars (so-called "Synthetic hegemonic currency" (SHC)). Mr Carney said that a "Synthetic Hegemonic Currency" (SHC) governed by the public sector and backed by a number of central bank digital currencies could replace the US dollar as the global reserve currency, and that this would be preferable to the alternatives, such as the Chinese Yuan/Renminbi becoming the global reserve.

Question 13. In your opinion, what are the most important risks related to "stablecoins"? Please rate from 1 (factor not relevant at all) to 5 (very relevant factor)

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

13.1 Is there any other important risks related to "stablecoins" not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a

13.2 Please explain in your answer potential differences in terms of risks between "stablecoins" and 'global stablecoins': *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a

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

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

Yes
No
Don't know / no opinion / not relevant

14.1 Please explain your reasoning for your answer to question 14: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Legislation should be technology agnostic / neutral.

Question 15. What is your experience (if any) as regards national regimes on crypto-assets? Please indicate which measures in these national laws are, in your view, an effective approach to crypto-assets regulation, which ones rather not. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We observe activities of various EU Member States as well as worldwide. Especially as a European community of states, based on common values, we prefer a common and coordinated approach.

Below some examples.

In November 2019, the German Parliament passed a bill* which amends an existing anti-money laundering directive to allow German banks to both sell and store cryptocurrencies. The new law took effect January 1, 2020, though certain requirements must first be met through the country's financial regulator.

*) Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie [https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2019-12-19-Gesetz-4-EU-Geldwaescherichtlinie/3-Verkuendetes-Gesetz.pdf]

In France, one of the main provisions of the PACTE law – entered into force in December 2019, relates to ICOs and Digital Asset Service Providers (DASPs). The law allows both enough flexibility for entrepreneurs to develop their ideas – in particular through the optional nature of a licence – and an appropriate level of protection for investors, thanks to the supervision of the French Markets Authority. The licence reflects both recognition of reliability and protection both for investors and issuers. The French Markets Authority is the single point of contact for ICO issuers and DASPs and the sole competent body for granting the licence. The French Markets Authority publishes a list of registered service providers and of ICOs which received its licence on its website, making this regime attractive for industry players as well as investors and consumers.

In Austria, virtual currency service providers are regulated under the Financial Markets Anti-Money Laundering Act* and have to be registered at the Austrian Financial Market Authority. Whereas ICOs depending on the design may constitute a financial service subject to a concession or may be covered by another investor protection law. Entities planning ICO activities shall therefore refer to the instructions of the Austrian Financial Market Authority and can contact the FinTech unit**.

*) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009769

**) https://www.fma.gv.at/querschnittsthemen/fintechnavigator/initial-coin-offering/

Question 16. In your view, how would it be possible to ensure that a bespoke regime for crypto-assets and crypto-asset service providers is proportionate to induce innovation, while protecting users of crypto-assets? Please indicate if such a bespoke regime should include the abovementioned categories (payment, investment and utility tokens) or exclude some of them, given their specific features (e.g. utility tokens). *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Concerning whether a bespoke regime should include the abovementioned categories or exclude some of them, we believe that a bespoke regime should only be foreseen for utility tokens for consumer protection.

We believe that the introduction of a license (which would only relate to assets which are not regulated by PSD2/EMD2 and MIFID, i.e. utility tokens), such as the license delivered by the French Markets Authority, delivered by a EU authority and whose implementation is delegated to national competent authorities, would allow to induce innovation while ensuring the appropriate level of protection for users of these crypto-assets.

Question 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 (See the discussion paper of the Basel Committee on Banking Supervision (BCBS))?

Yes
No
Don't know / no opinion / not relevant

17.1 Please explain your reasoning for your answer to question 17: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 17 is not clear or not well-formulated.

Question 18. Should harmonisation of national civil laws be considered to provide clarity on the legal validity of token transfers and the tokenisation of tangible (material) assets? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method

We think that first of all a European Securities Law Legislation and insolvency rights would be required.

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

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

Question 19. Can you indicate the various types and the number of service providers related to crypto-assets (issuances of crypto-assets, exchanges, trading platforms, wallet providers, ...) in your jurisdiction? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

This question is not really for an association; however we can provide some examples in countries where our members operate.

In Germany, crypto-assets ("Krypto-Werte") entered into force in January 2020*, thus there is no current experience on the matter for the time being. (*) Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie [https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2019-12-19-Gesetz-4-EU-Geldwaescherichtlinie/3-Verkuendetes-Gesetz.pdf]

In France, the PACTE law has created the DASP status which allows actors to provide the following services on digital assets (crypto currency and utility tokens): custody of digital assets, meaning in practice the custody of cryptographic keys on behalf of a client; the service of buying or selling digital assets for legal tender; the service of trading digital assets for other digital assets; the reception and transmission of orders for digital assets, meaning the act of receiving and transmitting buy or sell orders for digital assets on behalf of a client; the management of digital asset portfolios, meaning the act of managing, on a discretionary, client-by-client basis, portfolios that include one or more digital assets under a mandate given by a client; advice to investors in digital assets. This means giving personalised recommendations to a third party, either at their request or on the initiative of the service provider providing the advice, concerning one or more digital assets; digital asset underwriting, meaning the act of purchasing digital assets directly from a digital asset issuer, with a view to subsequently selling them; the guaranteed investment of digital assets, which consists in searching for buyers on behalf of a digital asset issuer and guaranteeing them a minimum amount of purchases by undertaking to buy any digital assets that are not placed; the unsecured investment of digital assets, meaning the act of searching for buyers on behalf of a digital asset issuer without guaranteeing them an amount of purchases; and the operation of a trading platform for digital assets. This concerns the management of one or more digital asset trading platforms, within which multiple buying and selling interests expressed by third parties for digital assets in exchange for other digital assets or a currency that is legal tender can interact in such a way as to result in the conclusion of contracts. This law has entered into force in December 2019 and thus so far we are not aware of any service providers who comply with the above regime, keeping in mind that there were already service providers that had operated some of these services without the license.

In Finland and from 1 November 2019, only virtual currency providers who fulfill the requirements provided by national legislation may practice activities in Finland. In Finland there are five service providers currently registered to the Finnish Financial Services Authority. Unauthorised provision of virtual currencies is prohibited in Finland and subject to a fine. https://www.finanssivalvonta.fi/en/publications-and-press-releases/Press-release/2019/the-financial-supervisory-authority-granted-five-registrations-as-virtual-currency-provider--scope-of-supervision-is-the-prevention-of-money-laundering2/

In Austria, as of 10 January 2020 only virtual currency service providers (VCSP) who fulfill the requirements of the local legislation are allowed to practice their activities in Austria. VCSPs are regulated under the Financial Markets Anti-Money Laundering Act* and consist of all service providers offering one or more of the following services: (a) services to secure private cryptographic keys in order to hold, store and transfer virtual currencies on behalf of a customer (electronic wallet providers); (b) exchange of virtual currencies in fiat money and vice versa; (c) exchange of one or more virtual currencies with each other; (d) transfer of virtual currencies; (e) provision of financial services for the issuance and sale of virtual currencies. (*) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009769

1. Issuance of crypto-assets

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

1.1. Issuance of crypto-assets in general

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

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

Yes

No

Don't know / no opinion / not relevant

20.1 Please explain your reasoning for your answer to question 20: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe in principle for functional and consumer protection reasons it is not necessary that the issuer or sponsor of crypto-assets marketed to EU investors/consumers should be established or have a physical presence in the EU as any financial instrument marketed to EU investors / consumers falls under European regulation. It is first important to distinguish: 1) law under which issuance is made 2) marketing to EU consumers means compliance to EU legislation.

This is in as far as it concerns the offering of the tokens as a financial instrument only but if the issuance involves an infrastructural function then it would make sense that the provider of this infrastructure has a European presence in line with what is expected in the case securities settlement infrastructures.

Question 21. Should an issuer or a sponsor of crypto-assets be required to provide information (e.g. through a 'white paper') when issuing crypto-assets?

Yes

No

This depends on the nature of the crypto-asset (utility token, payment token, hybrid token, ...)
Don't know / no opinion / not relevant

Question 21.1 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 crypto-assets, on the secondary trading, the underlying technology, potential conflicts of interest, ...): *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that the responsibility for the disclosure as well as the content of the information should be those defined in EU legislation, e.g. MiFID II and other relevant regulations (from UCITS-V to CRDS).

Question 22. If a requirement to provide the information on the offers of crypto-assets is imposed on their issuer/sponsor, would you see a need to clarify the interaction with existing pieces of legislation that lay down information requirements (to the extent that those rules apply to the offers of certain crypto-assets, such as utility and/or payment tokens)? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)
The Consumer Rights Directive			X		
The E-Commerce Directive			X		
The EU Distance Marketing of Consumer Financial Services Directive			X		

22.1 Is there any other existing piece of legislation laying down information requirements with which the interaction would need to be clarified? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Especially MiFID II and potentially the Undertakings for the Collective Investment in Transferable Securities Directive (UCITS V) or Alternative Investment Fund Managers Directive (AIFMD). But also the Prospectus/PRIIPS – depending on the use case.

22.2 Please explain your reasoning and indicate the type of clarification (legislative/non legislative) that would be required: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

General compliance to existing regulation as mentioned in our answer to Question 22.1 is necessary.

Question 23. Beyond any potential obligation as regards the mandatory incorporation and the disclosure of information on the offer, should the crypto-asset issuer or sponsor be subject to other requirements? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know /no opinion /not relevant
The managers of the issuer or sponsor should be subject to fitness and probity standards					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	

23.1 Is there any other requirement not mentioned above to which the crypto-asset issuer should be subject? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We would also add the sustainable finance disclosure requirements.

23.2 Please explain your reasoning for your answers to question 23: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As said in our answer to Question 22.2, we would recommend general compliance to existing regulation.

1.2. Issuance of "stablecoins" backed by real assets

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

Question 24. In your opinion, what would be the objective criteria allowing for a distinction between "stablecoins" and "global stablecoins" (e.g. number and value of "stablecoins" in circulation, size of the reserve, ...)? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that first of all stablecoins have to be defined either as simple promise or legal claim (E-money) or collective investment (UCITS or AIFM).

Question 25.1 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 "stablecoins" if each is proposal is relevant.

	Relevant	Not relevant	Don't know /no opinion
The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)			
The issuer should contain the creation of "stablecoins" so that it is always lower or equal to the value of the funds of the reserve			

The assets or funds of the reserve should be segregated from the issuer's balance sheet			
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)			
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)			
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating			
Obligation for the assets or funds to be held in custody with credit institutions in the EU			
Obligation for the assets or funds to be held for safekeeping at the central bank			
Periodic independent auditing of the assets or funds held in the reserve			
The issuer should disclose information to the users on (i) how it intends to provide stability to the "stablecoins", (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve			
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically			
Obligation for the issuer to use open source standards to promote competition			
Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer			

25.1 a) Is there any other requirements not mentioned above that could be imposed on "stablecoins" issuers and/or the manager of the reserve? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A "reserve" is a no defined term, the issue is the legal liability.

We believe that stablecoins and in particular global stablecoins might have to be asked to meet certain additional governance requirements to ensure for example some geographical balance. Additionally, Europe's crypto-asset framework should consider how the present discussion on integrating ESG principles into the financial value chain could apply to stablecoins.

25.1 b) Please Please illustrate your responses to question 25.1: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that first of all stablecoins have to be defined either as simple promise or legal claim (E-money) or collective investment (UCITS or AIFM).

We would like to comment on two entries of the table in Question 25.1. Concerning the entry "the assets of the reserve should not be encumbered (i.e. not pledged as collateral)", we think that the question is not clear (should not be pledged externally but should be used as collateral for the stable coin).

Concerning the entry "The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)", we would like to specify that the issuer of the reserve should be subject to prudential requirements only for operational risk coverage.

Question 25.2 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 "global stablecoins" if each is proposal is relevant.

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

25.2 a) Is there any other requirements not mentioned above that could be imposed on "stablecoins" issuers and/or the manager of the reserve? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A "reserve" is a no defined term, the issue is the legal liability.

We would suggest to have a look at the ECB oversight requirements for retail payment systems.

25.2 b) Please Please illustrate your responses to question 25.2: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that first of all stablecoins have to be defined either as (1) simple promise of market making/ repayment or (2) legal claim against the issuer (E-money) or (3) collective investment with asset kept at a custodian/depositary (UCITS or AIFM).

"Stablecoins" could be used by anyone (retail or general purpose) or only by a limited set of actors, i.e. financial institutions or selected clients of financial institutions (wholesale). The scope of uptake may give rise to different risks. The G7 report on "investigating the impact of global stablecoins" stresses that "*Retail stablecoins, given their public*

nature, likely use for high-volume, small-value payments and potentially high adoption rate, may give rise to different risks than wholesale stablecoins available to a restricted group of users".

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

Yes
No
Don't know / no opinion / not relevant

26.1 Please explain your reasoning for your answer to question 26: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We welcome uniform standards in the member states. Differentiation in the B2B and B2C sectors can help to realise efficiency gains.

We would suggest to investigate aligning the approach with those of the ECB oversight requirements for payment systems, which distinguishes between different classes of payment systems depending on their systemic importance, market penetration etc.

2. Trading platforms

Trading platforms function as a market place bringing together different crypto-asset users that are either looking to buy or sell crypto-assets. Trading platforms match buyers and sellers directly or through an intermediary. The business model, the range of services offered and the level of sophistication vary across platforms. Some platforms, so-called 'centralised platforms', hold crypto-assets on behalf of their clients while others, so-called decentralised platforms, do not. Another important distinction between centralised and decentralised platforms is that trade settlement typically occurs on the books of the platform (off-chain) in the case of centralised platforms, while it occurs on DLT for decentralised platforms (on-chain). Some platforms have already adopted good practice from traditional securities trading venues while others use simple and inexpensive technology.

Question 27. In your opinion and beyond market integrity risks (see section III. C. 1. below), what are the main risks in relation to trading platforms of crypto-assets? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

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

Losses of users' crypto-assets through theft or hacking (cyber risks)						
Lack of procedures to ensure fair and orderly trading						
Access to the trading platform is not provided in an undiscriminating way						
Delays in the processing of transactions						
For centralised platforms: Transaction settlement happens in the book of the platform and not necessarily recorded on DLT. In those cases, confirmation that the transfer of ownership is complete lies with the platform only (counterparty risk for investors vis-à-vis the platform)						
Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse						

27.1 Is there any other main risks posed by trading platforms of crypto-assets not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Regulation of trading platforms should be technology agnostic.

27.2 Please explain your reasoning for your answer to question 27: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Trading venues are regulated in MiFID II. The MIFID II rules for trading venues should apply to crypto-asset trading venues as well. The table does not fit to definition in MiFiD II etc., therefore we decided to leave the table empty.

Question 28. What are the requirements that could be imposed on trading platforms in order to mitigate those risks? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)
Trading platforms should have a physical presence in the EU					
Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					
Trading platforms should segregate the assets of users from those held on own account					
Trading platforms should be subject to rules on conflicts of interest					
Trading platforms should be required to keep appropriate records of users' transactions					
Trading platforms should have an adequate complaints handling and redress procedures					
Trading platforms should be subject to prudential requirements (including capital requirements)					
Trading platforms should have adequate rules to ensure fair and orderly trading					

Trading platforms should provide access to its services in an undiscriminating way					
Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse					
Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)					
Trading platforms should be responsible for screening crypto-assets against the risk of fraud					

28.1 Is there any other requirement that could be imposed on trading platforms in order to mitigate those risks? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Trading venues are regulated in MiFID II. The MIFID II rules for trading venues should apply to crypto-asset trading venues as well. AMLD V already imposes AML requirements. The table does not fit to definition in MiFiD II etc., therefore we decided to leave the table empty.

With a view to preventing fraud, possible blocking periods should be sought for the exchange of crypto-assets in third countries.

Finally, requirements to be able to trace transactions as per Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 should be considered.

28.2 Please indicate if those requirements should be different depending on the type of crypto-assets traded on the platform and explain your reasoning for your answers to question 28: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Typically, trading is either FX (= PSD2/EMD2) or venue for financial instruments (= MiFID II, etc.).

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

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

Question 29. In your opinion, what are the main risks in relation to crypto-to-crypto and fiat–to-crypto exchanges? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know /no opinion /not relevant
Absence of accountable entity in the EU						

Lack of adequate governance arrangements, including operational resilience and ICT security						
Conflicts of interest arising from other activities						
Absence/inadequate recordkeeping of transactions						
Absence/inadequate complaints or redress procedures are in place						
Bankruptcy of the exchange						
Inadequate own funds to repay the consumers						
Losses of users' crypto-assets through theft or hacking						
Users suffer loss when the exchange they interact with does not exchange crypto-assets against fiat currency (conversion risk)						
Absence of transparent information on the crypto-assets proposed for exchange						

29.1 Is there any other main risks in relation to crypto-to-crypto and fiat–to-crypto exchanges not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The main risks in the crypto-to-crypto and fiat-to-crypto exchanges are the possibility of concealing payment flows, money laundering, tax evasion and the associated financing of illegal activities, terrorism and military equipment.

29.2 Please explain your reasoning for your answer to question 29: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Depending on the type of financial instrument (payment/FX/securities) there should be no difference to existing financial services providers concerning KYC, AML/CFT, etc.

Question 30. What are the requirements that could be imposed on exchanges in order to mitigate those risks? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

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

Exchanges should be subject to prudential requirements (including capital requirements)						
Exchanges should be subject to advertising rules to avoid misleading marketing/promotions						
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)						
Exchanges should be responsible for screening crypto-assets against the risk of fraud						

30.1 Is there any other requirement that could be imposed exchanges in order to mitigate those risks? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

30.2 Please indicate if those requirements should be different depending on the type of crypto-assets available on the exchange and explain your reasoning for your answers to question 30: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Depending on the type of financial instrument (payment/FX/securities) there should be no difference to existing financial services providers concerning KYC, AML/CFT, etc.

4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys 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. 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.

Question 31. In your opinion, what are the main risks in relation to the custodial wallet service provision? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know /no opinion /not relevant
No physical presence in the EU						
Lack of adequate governance arrangements, including operational resilience and ICT security						
Absence or inadequate segregation of assets held on the behalf of clients						
Conflicts of interest arising from other activities (trading, exchange)						

Absence/inadequate recordkeeping of holdings and transactions made on behalf of users						
Absence/inadequate complaints or redress procedures are in place						
Bankruptcy of the custodial wallet provider						
Inadequate own funds to repay the consumers						
Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)						
The custodial wallet is compromised or fails to provide expected functionality						
The custodial wallet provider behaves negligently or fraudulently						
No contractual binding terms and provisions with the user who holds the wallet						

31.1 Is there any other risk in relation to the custodial wallet service provision not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

31.2 Please explain your reasoning for your answer to question 31: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method

We do not feel the need to fill out the table under Question 31 because custodial wallet services are either bank accounts, e-money accounts or securities accounts and existing regulation should apply.

Question 32. What are the requirements that could be imposed on custodial wallet providers in order to mitigate those risks? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know /no opinion /not relevant
Custodial wallet providers should have a physical presence in the EU						
Custodial wallet providers should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)						
Custodial wallet providers should segregate the asset of users from those held on own account						
Custodial wallet providers should be subject to rules on conflicts of interest						
Custodial wallet providers should be required to keep appropriate records of users' holdings and transactions						
Custodial wallet providers should have an adequate complaints handling and redress procedures						

Custodial wallet providers should be subject to capital requirements						
Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions						
Custodial wallet providers should be subject to certain minimum conditions for their contractual relationship with the consumers/investors						

32.1 Is there any other requirement that could be imposed on custodial wallet providers in order to mitigate those risks? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

32.2 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 for your answer to question 32: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We do not feel the need to fill out the table under Question 32 because custodial wallet services are either bank accounts, e-money accounts or securities accounts and existing regulation should apply.

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

Yes
No
Don't know / no opinion / not relevant

33.1 Please explain your reasoning for your answer to question 33: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Custodial wallet providers should be authorised to provide asset services under the same conditions as non-crypto asset providers. In addition, custodial wallet providers must be registered and licensed as per the Directive (EU) 2018/843 (AMLD V). As from January 2020, the list of obliged entities under AMLD V has been extended to virtual currency exchanges and custodian wallet providers. Therefore, such providers are already regulated. However, a "custodian wallet provider" is defined under AMLD V (art. 1 par. (2)(d)(19)) as an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies. This definition may not cover all the assets as defined under Question 33.

Question 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? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Please read our answer to Question 33.1.

5. Other services providers

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

Question 35. In your view, what are the services related to crypto-assets that should be subject to requirements? (When referring to execution of orders on behalf of clients, portfolio management, investment advice, underwriting on a firm commitment basis, placing on a firm commitment basis, placing without firm commitment basis, we consider services that are similar to those regulated by Annex I A of MiFID II.) Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know /no opinion /not relevant
Reception and transmission of orders in relation to crypto-assets						
Execution of orders on crypto-assets on behalf of clients						
Crypto-assets portfolio management						
Advice on the acquisition of crypto-assets						
Underwriting of crypto-assets on a firm commitment basis						
Placing crypto-assets on a firm commitment basis						
Placing crypto-assets without a firm commitment basis						
Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)						
Processing services, also known as 'mining' or 'validating' services in a DLT environment (e.g. 'miners' or validating 'nodes' constantly work on verifying and confirming transactions)						
Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)						
Services provided by developers that are responsible for maintaining/updating the underlying protocol						
Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)						

35.1 Is there any other services related to crypto-assets not mentioned above that should be subject to requirements? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Regulation should be technology agnostic and MiFID defines regulated services.

35.2 Please illustrate your response to question 35 by underlining the potential risks raised by these services if they were left unregulated and by identifying potential requirements for those service providers: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

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 , unless they qualify as electronic Payment Services Directive (PSD2) money. As a consequence, if

a firm proposes a payment service related to a crypto-asset (that do not qualify as e-money), it would fall outside the scope of PSD2.

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

Yes
No
Don't know / no opinion / not relevant

36.1 Please explain your reasoning for your answer to question 36: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Payment services are either regulated by PSD2 or by EMD2.

C. Horizontal questions

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

1. Market Integrity

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

Question 37. In your opinion, what are the biggest market integrity risks related to the trading of crypto-assets? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know /no opinion /not relevant
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		

37.1 Is there any other big market integrity risk related to the trading of crypto-assets not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

37.2 Please explain your reasoning for your answer to question 37: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Generally for all financial instruments a level playing field should be ensured. The principle "same business, same risk, same rules, same responsibility, same supervision" should apply.

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

Question 38. In your view, how should market integrity on crypto-asset markets be ensured? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

It should be ensured by applying the principles established in the MiFID II.

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

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

Yes
No
Don't know / no opinion / not relevant

If you see the need for supervisors to be able to formally identify the parties to transactions in crypto-assets, please explain explain how you would see this best achieved in practice: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We take it for granted that activities in the financial context can only be carried out by verified market participants. Implementation is guaranteed if the KYC requirements are also taken into account in the extended environment.

Depending on the function performed by the crypto-assets (see our answer to Question 7), the relevant existing identification standards should apply, e.g.:

- General KYC for non-payment function related assets; and
- in case of a crypto-asset with a payment function, beyond KYC, the existing requirements regarding 1) identification of the payer/payee (Regulation (EU) 2015/847 on information accompanying transfers of funds), 2) financial sanctions and embargos.

It is also important to say that crypto-asset transactions may be executed without traditional market participants (broker, etc.) and counterparties may be located outside the European Union.

39.1 Please explain your reasoning for your answer to question 39: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

Question 40. Provided that there are new legislative requirements to ensure the proper identification of transacting parties in crypto-assets, how can it be ensured that these requirements are not circumvented by trading on platforms/exchanges in third countries? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

This can never be excluded. But a reporting duty regarding volumes of trades could at least create transparency on activities.

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

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

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

Yes
No
Don't know / no opinion / not relevant

41.1 Please explain your reasoning for your answer to question 41: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

According to our opinion, "crypto-assets" should be the general term covering: (i) crypto-assets used as means of payments and (ii) crypto-assets used for investing (or for financing, vice versa) and (iii) utility token as "non-financial" functions such as e.g. lunch vouchers. As said in our answer to Question 7, we propose a classification based on intended functions.

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*". In addition, possible gaps may exist with regard to peer-to-peer transactions between private *assets* persons not acting as a business, in particular when done through wallets that are not hosted by custodial wallet providers.

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

Yes
No
Don't know / no opinion / not relevant

If you think there are crypto-asset services that should also be added to the EU AML/CFT legal framework obligations, describe the possible risks to tackle: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Service providers offering one or more of the following services should be added:
- Exchange of one or more virtual currencies with each other;
- transfer of virtual currencies; and
- provision of financial services for the issuance and sale of virtual currencies.

42.1 Please explain your reasoning for your answer to question 42: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.
We would add the above services due to the FATF supplementary recommendations published in October 2018.

Question 43. If a bespoke framework on crypto-assets is needed, do you consider that all crypto-asset service providers covered by this potential framework should become 'obliged entities' under the EU AML/CFT framework?
Yes
No
Don't know / no opinion / not relevant

43.1 Please explain your reasoning for your answer to question 43: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We replied "yes" as we believe that a bespoke framework on crypto-assets is needed to prevent that ML/TF/other sanction flows move from the regulated markets to the non regulated markets.

Question 44. In your view, how should the AML/CFT risks arising from peer-to-peer transactions (i.e. transactions without intermediation of a service provider) be mitigated? *5000 character(s) maximum* Including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Typically, there is always a service provider (exchanges, brokers, wallet providers) which should be under the AML/CFT, KYC and Regulation 2015/847 requirements.

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

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

Yes
No
Don't know / no opinion / not relevant

45.1 Please explain your reasoning for your answer to question 45: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe it will help clarifying the FATF Recommendations above mentioned.

Question 46. In your view, do you consider relevant that the following requirements are imposed as conditions for the registration and licensing of providers of services related to crypto-assets included in section III. B? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know /no opinion /not relevant
Information provided by the issuer of crypto-assets (the so-called 'white papers')				X		
Limits on the investable amounts in crypto-assets by EU consumers			X			
Information provided by the issuer of crypto-assets (the so-called 'white papers')				X		

46.1 Please explain your reasoning for your answer to question 46: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Similar obligations exist for regulated market participants performing similar functions/services, notably under MIFID/MIFIR. Regarding limits on consumer investment, the approach should be aligned with existing rules for other financial instruments that display similar risks to the consumer.

3. Consumer/investor protection

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. 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.

Question 47. What type of consumer protection measures could be taken as regards crypto-assets? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know /no opinion /not relevant
Information provided by the issuer of crypto-assets (the so-called 'white papers')						

Limits on the investable amounts in crypto-assets by EU consumers						
Suitability checks by the crypto-asset service providers (including exchanges, wallet providers, ...)						
Warnings on the risks by the crypto-asset service providers (including exchanges, platforms, custodial wallet providers, ...)						

47.1 Is there any other type of consumer protection measures that could be taken as regards crypto-assets? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We are of the opinion that the consumer protection measures should be the same as those regulated by MiFID II or UCITS V and AIFMD and prospectus. Some (utility) tokens that do not fall into the scope of transferable securities in MiFID II and/or UCITS or AIFMD should have same consumer protection measures as those mentioned in general consumer protection regulation, for example Consumer Protection Directive.

47.2 Please explain your reasoning for your answer to question 47 and indicate if those requirements should apply to all types of crypto assets or only to some of them: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The principle "same business, same risk, same rules, same responsibility, same supervision" should apply.

Question 48. Should different standards of consumer/investor protection be applied to the various categories of crypto-assets depending on their prevalent economic (i.e. payment tokens, stablecoins, utility tokens, ...) or social function?
Yes
No
Don't know / no opinion / not relevant

48.1 Please explain your reasoning for your answer to question 48: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We are of the opinion that different standards of consumer/investor protection should be applied to the various categories of crypto-assets depending on their prevalent economic or social function as it is today for payments (PSD2) and securities (MiFID II/UCITS V). Some (utility) tokens that do not fall into the scope of transferable securities in MiFID II and/or UCITS or AIFMD should have same consumer protection measures as those mentioned in general consumer protection regulation, for example Consumer Protection Directive.

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

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

Yes

No

Don't know / no opinion / not relevant

49.1 Please explain your reasoning for your answer to question 49: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We are of the opinion that different standards in terms of consumer/investor protection should be applied depending on whether the crypto-assets are bought in a public sale or in a private sale as it is for consumer protection in MiFID II and UCITS-V versus AIFMD (retail consumers versus professional investors). Some (utility) tokens that do not fall into the scope of transferable securities in MiFID II and/or UCITS or AIFMD should have same consumer protection measures for retail consumers as those mentioned in general consumer protection regulation.

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

Yes

No

Don't know / no opinion / not relevant

50.1 Please explain your reasoning for your answer to question 50: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Regulation and consumer protection do not depend on fees or business models. The existing consumer protection measures applicable to payment or investment services do not primarily focus on pricing of services/products but rather of the risks posed by the services/products. The same should be the case for crypto-assets.

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

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

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

51.1 Is there any other way the crypto-assets issued in third countries and that would not comply with EU requirements should be treated? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Every marketing of a financial services instrument to EU consumers requires compliance to EU legislation. This is independent from the problem how to enforce European law to non-European entities.

How to deal with these crypto-assets that would not comply with EU law would have to be looked at on a case by case basis depending on whether there is a clear legal entity behind it or not.

51.2 Please explain your reasoning for your answer to question 51: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

4. Supervision and oversight of crypto-assets service providers

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

Question 52. Which, if any, crypto-asset service providers included in Section III. B do you think should be subject to supervisory coordination or supervision by the European Authorities (in cooperation with the ESCB supervision by the European Authorities (in cooperation with the ESCB where relevant)? Please explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We are of the opinion that crypto-asset service providers included in Section III. B should be subject to supervisory coordination or supervision by the European Authorities as defined in the PSD2/EMD and MiFID II/UCITS V.

Question 53. Which are the tools that EU regulators would need to adequately supervise the crypto-asset service providers and their underlying technologies? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The tools should be the same as those defined in the PSD2/EMD2 and MiFID II/UCITS V.

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 would be captured by MiFID provisions. Consequently, firms providing services concerning security tokens should ensure they have the relevant MiFID authorisations and that they follow the relevant rules and requirements. MiFID is a cornerstone of the EU regulatory framework as financial instruments covered by MiFID are also subject to other financial legislation such as CSDR or EMIR, which therefore equally apply to post-trade activities related to security tokens. Building on ESMA's advice on crypto-assets and ICOs issued in January 2019 and on a preliminary legal assessment carried out by Commission services on the applicability and suitability of the existing EU legislation (mainly at level 1) 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, with none of them having been admitted to trading or traded on a trading venue nor admitted in a CSD book-entry system. 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. Such activities would be overseen by a central body or operator, de facto similarly to traditional market infrastructures such as multilateral trading venues or central security depositories. Based on the limited evidence currently available from the industry, it seems that activities related to security tokens would most likely develop via authorised centralised solutions. This could be driven by the relative efficiency gain that the use of the legacy technology of a central provider can generally guarantee (with near-instantaneous speed and high liquidity with large volumes), along with the business expertise of the central provider that would also ensure higher investor protection and easier supervision and enforcement of the rules. On the other hand, it seems that adjustment of existing EU rules would be required to allow for the development of permissionless networks and decentralised platforms where activities would not be entrusted to a central body or operator but would rather occur on a peer-to-peer 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 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 decentralized 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.

Question 54. Please highlight any recent market developments (such as issuance of security tokens, development or registration of trading venues for security tokens, ...) as regards security tokens (at EU or national level)? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In the past there have been many attempts to fraudulent activities and/or factual avoidance of existing legislation. We are of the opinion that the more tokens fall under legislation, the less the interest of issuers is.

Question 55. Do you think that DLT could be used to introduce efficiencies or other benefits in the trading, post-trade or asset management areas?
Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

If you agree with question 55, please indicate the specific areas where, in your opinion, the technology could afford most efficiencies when compared to the legacy system: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

55.1 Please explain your reasoning for your answer to question 55: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Efficiency expected in the post-trade area due to avoidance of re-conciliation will be balanced by additional technical resources (for distributed ledgers/databases) and new technology will not be (fully) compatible to legacy leading to parallel systems landscapes.

Question 56. Do you think that the use of DLT for the trading and post-trading of financial instruments poses more financial stability risks when compared to the traditional trading and post-trade architecture?
Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

56.1 Please explain your reasoning for your answer to question 56: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We selected "neutral" as we believe that the use of DLT for the trading and post-trading of financial instruments poses potential operational risks as any other new technology.

Question 57. Do you consider that DLT will significantly impact the role and operation of trading venues and post-trade financial market infrastructures (CCPs, CSDs) in the future (5/10 years' time)? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Trading venues and post-trade financial market infrastructures are based on a business function not technology.
While technology might generate efficiency, it does not change roles and responsibilities.

Question 58. Do you agree that a gradual regulatory approach in the areas of trading, post-trading and asset management concerning security tokens (e.g. provide regulatory guidance or legal clarification first regarding permissioned centralised solutions) would be appropriate?
Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

58.1 Please explain your reasoning for your answer to question 58: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 58 is unclear. We believe that it is crucial to ensure that the regulatory framework remains fully technology-neutral. The principle "same business, same risk, same rules, same responsibility, same supervision" should apply.

B. Assessment of legislation applying to 'security tokens'

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

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

1.1 Financial instruments

Under MiFID, financial instruments are specified in Section C of Annex I. These are inter alia 'transferable securities', 'money market instruments', 'units in collective investment undertakings' and various derivative instruments. Under Article 4(1)(15), 'transferable securities' notably means those classes of securities which are negotiable on the capital market, with the exception of instruments of payment. There is currently no legal definition of security tokens in the EU financial services legislation. Indeed, in line with a functional and technologically neutral approach to different categories

of financial instruments in MiFID, where security tokens meet necessary conditions to qualify as a specific type of financial instruments, they should be regulated as such. However, the actual classification of a security token as a financial instrument is undertaken by National Competent Authorities (NCAs) on a case-by-case basis. In its Advice, ESMA indicated that in transposing MiFID into their national laws, the Member States have defined specific categories of financial instruments differently (i.e. some employ a restrictive list to define transferable securities, others use broader interpretations). As a result, while assessing the legal classification of a security token on a case by case basis, Member States might reach diverging conclusions. This might create further challenges to adopting a common regulatory and supervisory approach to security tokens in the EU. Furthermore, some 'hybrid' crypto-assets can have 'investment-type' features combined with 'payment-type' or 'utility-type' characteristics. In such cases, the question is whether the qualification of 'financial instruments' must prevail or a different notion should be considered.

Question 59. Do you think that the absence of a common approach on when a security token constitutes a financial instrument is an impediment to the effective development of security tokens?
Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

59.1 Please explain your reasoning for your answer to question 59: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A common understanding of the minimum requirements for security tokens is important. Without this there can be no common trust in the representation of the financial instrument. Moreover and as explained in the introduction "1.1 Financial instruments", the problem arises from heterogeneous implementation across Europe, not from the technology. It is important to gain agreement on a classification of a financial instrument in general first.

Question 60. If you consider that the absence of a common approach on when a security token constitutes a financial instrument is an impediment, what would be the best remedies according to you? Please rate from 1 (factor not relevant at all) to 5 (very relevant factor)

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

60.1 Is there any other solution that would be the best remedies according to you? *5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that other solutions possible could be:

- Existence of a European Securities Law Legislation.
- Independent pure technical standard i.e. by ISO.

60.2 Please explain your reasoning for your answer to question 60: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A common understanding of the minimum requirements for security tokens is important. Without this there can be no common trust in the representation of the financial instrument. Moreover and as explained in the introduction "1.1 Financial instruments", the problem arises from heterogeneous implementation across Europe, not from the technology. It is important to gain agreement on a classification of a financial instrument in general first.

Question 61. How should financial regulators deal with hybrid cases where tokens display investment-type features combined with other features (utility-type or payment-type characteristics)? Please rate from 1 (factor not relevant at all) to 5 (very relevant factor)

	1 (factor not relevant at all)	2	3	4	5 (very relevant factor)	Don't know /no opinion /not relevant
Hybrid tokens should qualify as financial instruments/security tokens	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					

61.1 Is there any other way financial regulators should deal with hybrid cases where tokens display investment-type features combined with other features? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

61.2 Please explain your reasoning for your answer to question 61: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We indicated "1" as we think that hybrid tokens should not be considered in the classification of crypto-assets to avoid uncertainties or grey zones. See also our answer under Question 7.

1.2. Investment firms

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

Question 62. Do you agree that existing rules and requirements for investment firms can be applied in a DLT environment?
Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

62.1 Please explain your reasoning for your answer to question 62: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

MiFID II is technology agnostic/neutral and can be applied in a DLT environment.

Question 63. Do you think that a clarification or a guidance on applicability of such rules and requirements would be appropriate for the market?
Completely agree
Rather agree
Neutral
Rather disagree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

63.1 Please explain your reasoning for your answer to question 63: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

MiFID II is technology agnostic/neutral and can be applied in a DLT environment.

1.3 Investment services and activities

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

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

Don't know / no opinion / not relevant

64.1 Please explain your reasoning for your answer to question 64: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

MiFID II is technology agnostic/neutral and can be applied in a DLT environment.

Question 65. Do you consider that the transposition of MiFID II into national laws or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT for investment services and activities? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No, we don't think that the transposition of MiFID II into national laws would facilitate or otherwise prevent the use of DLT for investment services and activities.

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 , platforms which would engage in trading of security tokens may reported by ESMA in its advice fall under three main broad categories as follows: Platforms with a central order book and/or matching orders would qualify as multilateral systems; Operators of platforms dealing on own account and executing client orders against their proprietary capital, would not qualify as multilateral trading venues but rather as investment firms; and Platforms that are used to advertise buying and selling interests and where there is no genuine trade execution or arranging taking place may be considered as bulletin boards and fall outside of MiFID II scope (recital 8 of MiFIR).

Question 66. Would you see any particular issues (legal, operational) in applying trading venue definitions and requirements related to the operation and authorisation of such venues to a DLT environment which should be addressed? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No, we don't see any particular issues (legal, operational) in applying trading venue definitions and requirements related to the operation and authorization of such venues to a DLT environment. As trading venues are covered by MiFID II and ESMA advice.

1.5. Investor protection

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

Question 67. Do you think that current scope of investor protection rules (such as information documents and the suitability assessment) are appropriate for security tokens? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Yes, we believe that the current scope of investor protection rules (such as information documents and the suitability assessment) are appropriate for security tokens. We believe that the principle "same business, same risk, same rules, same requirements" should apply.

Question 68. Would you see any merit in establishing specific requirements on the marketing of security tokens via social media or online? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't see any merit in establishing specific requirements on the marketing of security tokens via social media or online, as the requirements are for marketing (due to consumer protection) but independent from the technology.

Question 69. Would you see any particular issue (legal, operational) in applying MiFID investor protection requirements to security tokens? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't see any particular issue (legal, operational) in applying MiFID investor protection requirements to security tokens. We also think that UCITS V/AIFMD may be relevant too.

1.6. SME growth markets

To be registered as SME growth markets, MTFs need to comply with requirements under Article 33 (e.g. 50% of SME issuers, appropriate criteria for initial and ongoing admission, effective systems and controls to prevent and detect market abuse). SME growth markets focus on trading securities of SME issuers. The average number of transactions in SME securities is significantly lower than those with large capitalisation and therefore less dependent on low latency and high throughput. Since trading solutions on DLT often do not allow processing the amount of transactions typical for most liquid markets, the Commission is interested in gathering feedback on whether trading on DLT networks could offer cost efficiencies (e.g. lower costs of listing, lower transaction fees) or other benefits for SME Growth Markets that are not necessarily dependent on low latency and high throughput.

Question 70. Do you think that trading on DLT networks could offer cost efficiencies or other benefits for SME Growth Markets that do not require low latency and high throughput? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that trading on DLT networks won't offer cost efficiencies or other benefits for SME Growth Markets as every DLT system has a business model to be paid (example, brokers, miners/mining, pools, etc.). Today, the main costs for SMEs results from compliance to regulation, but not from the question of a certain technology (e.g. central database, distributed database, distributed ledger, 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 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.

Question 71. Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

This question is not very clear to us, as also regulated markets offers access to retail investors (via banks or brokers).

1.8. Admission of financial instruments to trading

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

Question 72. Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No, we don't see any particular issue (legal, operational) in applying the above requirements to security tokens.
Also in this case we believe that the principle "same business, same risk, same rules, same requirements, same responsibilities" should apply.

1.9 Access to a trading venues

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

Question 73. What are the risks and benefits of allowing direct access to trading venues to a broader base of clients? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Articles 53(3) and 19(2) of MiFID abovementioned reflect important elements of consumer protection, which should apply to every technology.

1.10 Pre and post-transparency requirements

In its Articles 3 to 11, MiFIR sets out transparency requirements for trading venues in relations to both equity and non-equity instruments. In a nutshell for equity instruments, it establishes pre-trade transparency requirements with certain waivers subject to restrictions (i.e. double volume cap) as well as post-trade transparency requirements with authorized deferred publication. Similar structure is replicated for non-equity instruments. These provisions would apply to security tokens. The availability of data could perhaps be an issue for best execution 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.

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

Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

74.1 Please explain your reasoning for your answer to question 74: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We think that pre- and post-transparency requirements are appropriate for security tokens as we are the opinion to once again applying the principle "same business, same risk, same rules, same requirements, same responsibilities".

Question 75. Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed (e.g. in terms of availability of data or computation of thresholds)? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No, we don't see any particular issue (legal, operational) in applying the above requirements to security tokens.
Also in this case the principle "same business, same risk, same rules, same requirements, same responsibilities" should apply.

1.11. Transaction reporting and obligations to maintain records

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

Question 76. Would you see any particular issue (legal, operational) in applying these requirement to security tokens which should be addressed? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't see any particular issue (legal, operational) in applying the abovementioned requirements to security tokens. Technically, DLT could provide some more efficiency but same rules should apply.

2. Market Abuse Regulation (MAR)

MAR establishes a comprehensive legislative framework at EU level aimed at protecting market integrity. It does so by establishing rules around prevention, detection and reporting of market abuse. The types of market abuse prohibited in MAR are insider dealing, unlawful disclosure of inside information and market manipulation. The proper application of the MAR framework is very important for guaranteeing an appropriate level of integrity and investor protection in the context of trading in security tokens. Security tokens are covered by the MAR framework where they fall within the scope of that regulation, as determined by its Article 2. Broadly speaking, this means that all transactions in security tokens admitted to trading or traded on a trading venue (under MiFID Article 4(1)(24) 'trading venue' means a regulated market (RM), a Multilateral Trading Facility (MTF) or an Organised Trading Facility (OTF')) are captured by its provisions, regardless of whether transactions or orders in those tokens take place on a trading venue or are conducted over-the-counter (OTC).

2.1. Insider dealing

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

Question 77. Do you think that the current scope of Article 8 of MAR on insider dealing is appropriate to cover all cases of insider dealing for security tokens? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that the current scope of Art. 8 of MAR on insider dealing is appropriate to cover all cases of insider dealing for security tokens, as it is not related to a certain technology.

2.2. Market manipulation

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

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

Question 78. Do you think that the notion of market manipulation as defined in Article 12 of MAR is sufficiently wide to cover instances of market manipulation of security tokens? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that the notion of market manipulation as defined in Art. 12 of MAR is sufficiently wide to cover instances of market manipulation of security tokens, as it is not related to a certain technology.

Question 79. Do you think that there is a particular risk that manipulative trading in crypto-assets which are not in the scope of MAR could affect the price or value of financial instruments covered by MAR? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

This question is not clear to us.

3. Short Selling Regulation (SSR)

The sets down rules that aim to achieve the following objectives: Short Selling Regulation (SSR) (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, 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 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.

Question 80. Have you detected any issues that would prevent effectively applying SSR to security tokens? Please rate from 1 (not a concern) to 5 (strong concern)

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know /no opinion /strong concern
Transparency for significant net short positions	X					
Restrictions on uncovered short selling	X					
Competent authorities' power to apply temporary restrictions to short selling	X					

80.1 Is there any other issue that would prevent effectively applying SSR to security tokens? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No.

80.2 Please explain your reasoning for your answer to question 80: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We haven't detected any issues that would prevent effectively applying SSR to security tokens as the SSR is not related to a certain technology.

Question 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? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We haven't 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, as this is not related to a certain technology.

4. Prospectus Regulation (PR)

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

4.1. Scope and exemptions

With the exception of out of scope situations and exemptions (Article 1(2) and (3)), the PR requires the publication of a prospectus before an offer to the public or an admission to trading on a regulated market (situated or operating within a Member State) of transferable securities as defined in MiFID II. The definition of 'offer of securities to the public' laid

down in Article 2(d) of the PR is very broad and should encompass offers (e.g. STOs) and advertisement relating to security tokens. If security tokens are offered to the public or admitted to trading on a regulated market, a prospectus would always be required unless one of the exemptions for offers to the public under Article 1(4) or for admission to trading on a RM under Article 1(5) applies.

Question 82. Do you consider that different or additional exemptions should apply to security tokens other than the ones laid down in Article 1(4) and Article 1(5) of PR?
Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

82.1 Please explain your reasoning for your answer to question 82: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't believe 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. Also in this case we would apply the principle "same business/same activities, same risk, same rules, same requirements, same responsibilities".

4.2. The drawing up of the prospectus
Delegated Regulation (EU) 2019/980, which lays down the format and content of all the prospectuses and its related documents, does not include schedules for security tokens. However, Recital 24 clarifies that, due to the rapid evolution of securities markets, where securities are not covered by the schedules to that Regulation, national competent authorities should decide in consultation with the issuer which information should be included in the prospectus. Such approach is meant to be a temporary solution. A long term solution would be to either (i) introduce additional and specific schedules for security tokens, or (ii) lay down 'building blocks' to be added as a complement to existing schedules when drawing up a prospectus for security tokens. The level 2 provisions of prospectus also defines the specific information to be included in a prospectus, including Legal Entity Identifiers (LEIs) and ISIN. It is therefore important that there is no obstacle in obtaining these identifiers for security tokens. The eligibility for specific types of prospectuses or relating documents (such as the secondary issuance prospectus, the EU Growth prospectus, the base prospectus for non-equity securities or the universal registration document) will depend on the specific types of transferable securities to which security tokens correspond, as well as on the type of the issuer of those securities (i.e. SME, mid-cap company, secondary issuer, frequent issuer). Article 16 of PR requires issuers to disclose risk factors that are material and specific to the issuer or the security, and corroborated by the content of the prospectus. ESMA's guidelines on risk factors under the PR assist national competent authorities in their review of the materiality and specificity of risk factors and of the presentation of risk factors across categories depending on their nature. The prospectus could include pertinent risks associated with the underlying technology (e.g. risks relating to technology, IT infrastructure, cyber security, etc, ...). ESMA's guidelines on risk factors could be expanded to address the issue of materiality and specificity of risk factors relating to security tokens.

Question 83. Do you agree that Delegated Regulation (EU) 2019/980 should include specific schedules about security tokens?
Yes
No
Don't know / no opinion / not relevant

83.1 Please explain your reasoning for your answer to question 83: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that the Delegated Regulation (EU) 2019/980 should not include specific schedules about security tokens. Also in this case we would apply the principle "same business/ activities, same risk, same rules, same requirements, same responsibilities".

Question 84. Do you identify any issues in obtaining an ISIN for the purpose of issuing a security token? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't identify any issues in obtaining an ISIN for the purpose of issuing a security token.

Question 85. Have you identified any difficulties in applying special types of prospectuses or related documents (i.e. simplified prospectus for secondary issuances, the EU Growth prospectus, the base prospectus for non-equity securities, the universal registration document) to security tokens that would require amending these types of prospectuses or related documents? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We haven't 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.

Question 86. Do you believe that an alleviated *ad hoc* 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
Don't know / no opinion / not relevant

86.1 Please explain your reasoning for your answer to question 86: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that an alleviated ad hoc prospectus type or regime should not be introduced. Also in this case we would apply the principle "same business, same risk, same rules, same requirements, same responsibilities".

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

Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

87.1 Please explain your reasoning for your answer to question 87: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We answered "Neutral" to Question 87 as we believe that in general regulation should be technology neutral / agnostic. However due to the novelty of this new technology (i.e. DLT), a clarification about the risks is needed in order to improve consumer protection.

5. Central Securities Depositories Regulation (CSDR)

CSDR aims to harmonise the timing and conduct of securities settlement in the European Union and the rules for central securities depositories (CSDs) which operate the settlement infrastructure. It is designed to increase the safety and efficiency of the system, particularly for intra-EU transactions. In general terms, the scope of the CSDR refers to the 11 categories of financial instruments listed under MiFID. However, various requirements refer only to subsets of categories under MiFID. Article 3(2) of CSDR requires that transferable securities traded on a trading venue within the meaning of MiFID II be recorded in book-entry form in a CSD. The objective is to ensure that those financial instruments can be settled in a securities settlement system, as those described by the Settlement Finality Directive (SFD). Recital 11 of CSDR indicates that CSDR does not prescribe any particular method for the initial book-entry recording. Therefore, in its advice, ESMA indicates that any technology, including DLT, could virtually be used, provided that this book-entry form is with an authorised CSD. However, ESMA underlines that there may be some national laws that could pose restrictions to the use of DLT for that purpose. There may also be other potential obstacles stemming from CSDR. For instance, the provision of 'Delivery versus Payment' settlement in central bank money is a practice encouraged by CSDR. Where not practical and available, this settlement should take place in commercial bank money. This could make the settlement of securities through DLT difficult, as the CSDR would have to effect movements in its cash accounts at the same time as the delivery of securities on the DLT. This section is seeking stakeholders' feedback on potential obstacles to the development of security tokens resulting from CSDR.

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

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know /no opinion /strong concern
Definition of 'central securities depository' and whether platforms can be authorised as a CSD operating a securities settlement system which is designated under the SFD	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					

88.1 Is there any other particular issue with applying the following definitions in a DLT environment Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No, we have no particular issues. Also in this case we would apply the principle "same business/ activities, same risk, same rules, same requirements, same responsibilities".

88.2 Please explain your reasoning for your answer to question 88: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Additionally, we want to point out that a "CSD" provides a legal and regulated function, which does not depend on the technology applied. Even by using DLT, for a public IPO a legally approved register would be needed, while a private issuance does not need this function – leading to two different equity instruments.

Question 89. Do you consider that the book-entry requirements under CSDR are compatible with security tokens?
Yes
No
Don't know / no opinion / not relevant

89.1 Please explain your reasoning for your answer to question 89: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We consider that the book-entry requirements under CSDR are compatible with security tokens. Also in this case we would apply the principle "same business, same risk, same rules, same requirements, same responsibilities".

Question 90. Do you consider that national law (e.g. requirement for the transfer of ownership) or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT solution? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't have a specific opinion on this as an answer would require an in-depth analysis on whether the various national law contain some not-technology-neutral parts.

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

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know /no opinion /strong concern
Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system	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					

91.1 Is there any other particular issue with applying the current rules in a DLT environment, (including other provisions of CSDR, national rules applying the EU acquis, supervisory practices, interpretation, applications...)?
Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

91.2 Please explain your reasoning for your answer to question 91: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Regulation, such as CSDR, should be technology agnostic/neutral.

Question 92. In your Member State, does your national law set out additional requirements to be taken into consideration, e.g. regarding the transfer of ownership (such as the requirements regarding the recording on an account with a custody account keeper outside a DLT environment)? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

6. Settlement Finality Directive (SFD)

The lays down rules to minimise risks related to transfers and payments Settlement Finality Directive 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.

Question 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 from 1 (not a concern) to 5 (strong concern)

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know /no opinion /strong concern
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					

93.1 Is there any other particular issue with applying the following definitions in the SFD or its transpositions into national law in a DLT environment? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that SFD should apply independent from the technology. However, public DLT (based on proof-of-work consensus) will have problems to comply, as there is no (legal) finality at all, but only a probabilistic "eventual consistency".

93.2 Please explain your reasoning for your answer to question 93: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Public DLT provides only "eventual consistency" (due to the proof-of-work consensus) but not finality when proof-of-work consensus is implemented.

Question 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 (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)? Please explain your reasoning. *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In private DLT, there is always a clearly defined location (based on the legal entity running the operations of the network and/or location of the initiative). Public DLT without defined legal responsibilities (and with unclear locations) do not qualify for SFD.

Question 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? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 / not relevant

96.1 Please explain your reasoning for your answer to question 96: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

7. Financial Collateral Directive (FCD)

The aims to create a clear uniform EU legal framework for the use of securities, Financial Collateral Directive 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.

Question 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 from 1 (not a concern) to 5 (strong concern)

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know /no opinion /strong concern

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

97.1 Is there any other particular issue with applying the following definitions in the FCD or its transpositions into national law in a DLT environment? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't know.

97.2 Please explain your reasoning for your answer to question 97: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 98. FCD sets out rules on conflict of laws. Would you see any particular issue with applying these rules in a DLT network? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't know.

Question 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? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

Question 100. Do you consider that the effective functioning and/or use of DLT solution is limited or constrained by any of the FCD provisions?
Yes
No
Don't know / no opinion / not relevant

100.1 Please explain your reasoning for your answer to question 100: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

8. European Markets Infrastructure Regulation (EMIR)
The applies to the central clearing, reporting and European Markets Infrastructure Regulation (EMIR) 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 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.

Question 101. Do you think that security tokens are suitable for central clearing?
Completely agree
Rather agree
Neutral
Rather disagree
Completely disagree
Don't know / no opinion / not relevant

101.1 Please explain your reasoning for your answer to question 101: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Currently no OTC token or EFT token exists.

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

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know /no opinion /strong concern
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					

102.1 Is there any other particular issue (including other provisions of EMIR, national rules applying the EU acquis, supervisory practices, interpretation, applications, ...) with applying the current rules in a DLT environment? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No, there is no other issue with applying the current rules in a DLT environment. We are of the opinion that the principle "same business / activities, same risk, same rules, same requirements, same responsibilities" should apply.

102.2 Please explain your reasoning for your answer to question 102: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

Question 103. Would you see the need to clarify that DLT solutions including permissioned blockchain can be used within CCPs or TRs? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We don't see the need to clarify that DLT solutions including permissioned blockchain can be used within CCPs or TRs, as especially permissioned DLT are simply databases or registers.

Question 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 *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

9. The Alternative Investment Fund Directive

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

Question 105. Do the provisions of the EU AIFMD legal framework in the following areas are appropriately suited for the effective functioning of DLT solutions and the use of security tokens? Please rate from 1 (not suited) to 5 (very suited)

	1 (not suited)	2	3	4	5 (very suited)	Don't know /no opinion /very suited
AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;					X	

AIFMD provisions requiring AIFMs to maintain and operate effective organisational and administrative arrangements, including with respect to identifying, managing and monitoring the conflicts of interest;					X	
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	

105.1 Is there any other area in which the provisions of the EU AIFMD legal framework are appropriately suited for the effective functioning of DLT solutions and the use of security tokens? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

105.2 Please explain your reasoning for your answer to question 105: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The principle "same business / activities, same risk, same rules, same requirements, same responsibilities" should apply.

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

Yes

No

Don't know / no opinion / not relevant

106.2 Please explain your reasoning for your answer to question 106: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The principle "same business, same risk, same rules, same requirements, same responsibilities" should apply.

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

The applies to UCITS established within the territories of the Member States and lays UCITS Directive 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 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.

Question 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 from 1 (not suited) to 5 (very suited)

	1 (not suited)	2	3	4	5 (very suited)	Don't know /no opinion /very suited
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	

107.1 Is there any other area in which the provisions of the EU UCITS Directive legal framework are appropriately suited for the effective functioning of DLT solutions and the use of security tokens? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

107.2 Please explain your reasoning for your answer to question 107: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The principle "same business / activities, same risk, same rules, same requirements, same responsibilities" should apply.

11. Other final comments and questions as regards tokens

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

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

Yes

No

Don't know / no opinion / not relevant

108.2 Please explain your reasoning for your answer to question 110: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that permissionless blockchain and decentralised platforms (in the sense of public DLT) should follow the same rules as other technologies, as legislation should be technology neutral / agnostic.
The principle "same business / activities, same risk, same rules, same requirements, same responsibilities" should apply.

Question 109. Which benefits and risks do you see in enabling trading or post-trading processes to develop on permissionless blockchains and decentralised platforms? *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

According to our opinion, it is fully unclear how "trading" should work on permissionless blockchain and decentralised platforms (in the sense of public DLT), i.e. without any "operator" being responsible for the matching of orders. A bilateral exchange between two participants using a "Blockchain" as a protocol layer would be an over-the-counter trade, while any "organized venue" would be an exchange etc. Benefits from DLT technology is doubtful and cannot be assessed for the time being.

Blockchain systems work in a fundamentally different way compared to the current trading and post-trading

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

Question 110. Do you think that the regulatory separation of trading and posttrading 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 / not relevant

110.2 Please explain your reasoning for your answer to question 112: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The "separation of trading and post-trading activities" defines roles and responsibilities, but is technology neutral / agnostic.

Question 111. Have you detected any issues beyond those raised in previous questions on specific provisions that would prevent effectively applying EU regulations to security tokens and transacting in a DLT environment, in particular as regards the objective of investor protection, financial stability and market integrity?
Yes
No
Don't know / no opinion / not relevant

111.1 Please provide specific examples and explain your reasoning for your answer to question 111: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

Question 112. Have you identified national provisions in your jurisdictions that would limit and/or constraint the effective functioning of DLT solutions or the use of security tokens?
Yes
No
Don't know / no opinion / not relevant

112.1 Please provide specific examples (national provisions, implementation of EU acquis, supervisory practice, interpretation, application, ...) and explain your reasoning for your answer to question 112: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

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 sets out the rules e-money directive (EMD2) for the business practices and supervision of e-money institutions. In its advice on crypto-assets, the EBA noted that national competent authorities reported a handful of cases where payment tokens could qualify as e-money, e.g. tokens pegged to a given currency and redeemable at par value at any time. Even though such cases may seem limited, there is merit in ensuring whether the existing rules are suitable for these tokens. In that this section, payments tokens, and more precisely "stablecoins", that

qualify as e-money are called 'e-money tokens' for the purpose of this consultation. Consequently, firms issuing such e-money tokens should ensure they have the relevant authorisations and follow requirements under EMD2. Beyond EMD2, payment services related to e-money tokens would also be covered by the Payment Services Directive (PSD2). PSD2 puts in place comprehensive rules for payment services, and payment transactions. In particular, the Directive sets out rules concerning a) strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud; b) the transparency of conditions and information requirements for payment services; c) the rights and obligations of users and providers of payment services. The purpose of the following questions is to seek stakeholders' views on the issues they could identify for the application of the existing regulatory framework to e-money tokens.

Question 113. Have you detected any issue in EMD2 that could constitute impediments to the effective functioning and/or use of e-money tokens?
Yes
No
Don't know / no opinion / not relevant

113.1 Please provide specific examples (EMD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application, …) and explain your reasoning for your answer to question 113: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.
N/a.

Question 114. Have you detected any issue in PSD2 which would constitute impediments to the effective functioning or use of payment transactions related to e-money token?
Yes
No
Don't know / no opinion / not relevant

114.1 Please provide specific examples (PSD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application, …) and explain your reasoning for your answer to question 114: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

Question 115. In your view, do EMD2 or PSD2 require legal amendments and/or supervisory guidance (or other non-legislative actions) to ensure the effective functioning and use of e-money tokens?
Yes
No
Don't know / no opinion / not relevant

115.1 Please provide specific examples and explain your reasoning for your answer to question 115: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that the principle "same business / activities, same risk, same rules, same requirements, same responsibilities" should apply. However, some improvements independent from "tokenisation" are possible, e.g. in EMD with higher limits and in PSD2 with an adoption to automated payment processes.

Under EMD2, 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*". As some *which is accepted by a natural or legal person other than the electronic money issuer* "stablecoins" with global reach (the so-called "global stablecoin") may qualify as e-money, the requirements under EMD2 would apply. Entities in

a "global stablecoins" arrangement (that qualify as e-money under EMD2) could also be subject to the provisions of PSD2. The following questions aim to determine whether the EMD2 and/or PSD2 requirements would be fit for purpose for such "global stablecoins" arrangements that could pose systemic risks.

Question 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 from 1 (completely inappropriate to 5 (completely appropriate)

	1 (completely inappropriate)	2	3	4	5 (completely appropriate)	Don't know /no opinion /very suited
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

116.1 Is there any other requirement under EMD2 that would be appropriate for "global stablecoins"? Please specify which one(s) and explain your reasoning: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

N/a.

116.2 Please explain your reasoning for your answer to question 116: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As EMD2 (and similarly PSD2) is a European directive and especially focused on consumer protection for retail customers. Therefore, it does not apply to any "global" solution, which would require a political discussion about a "global currency" regime. For so-called "stablecoins" in general, it is absolutely unclear for the time being, what they are: (i) only a marketing label and "promise" for a market-making, or (ii) E-Money as defined in EMD2, or (iii) some kind of "tokenised" money market fund with assets kept at a custodian/depositary as defined in UCITS V / AMFID. In the second case of "E-Money" with a legal claim against the issuer, EMD2 could be a blueprint for a global perspective. However, it has to be asked what features would define some token/coin as "global". Taking "Libra" as an example, it would be issued by an organisation under Swiss law and it - per jure - a "Swiss coin". As long as there is neither a "global payment directive" nor a super-national organisation as issuer (comparable to IMF with the SDR), there is no legal regime for a "global coin". See also the G7 Working Group on Stable Coin paper "Investigating the impact of global stablecoins" (Oct. 2019).

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

Rather disagree
Completely disagree
Don't know / no opinion / not relevant

117.1 Please explain your reasoning for your answer to question 117: *5000 character(s) maximum* including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

See our answer to Question 116.2 above.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser, Retail Banking and Consumer Policy (chiara.delloro@eacb.coop)