

Public consultation an EU framework for markets in crypto-assets

Fields marked with * are mandatory.

Introduction

This consultation is also available in [German](#) and [French](#).

Background for this public consultation

As stated by President von der Leyen in her political guidelines for the new Commission, it is crucial that Europe grasps all the potential of the digital age and strengthens its industry and innovation capacity, within safe and ethical boundaries. Digitalisation and new technologies are significantly transforming the European financial system and the way it provides financial services to Europe's businesses and citizens. Almost two years after the Commission adopted the [Fintech action plan in March 2018](#)¹, the actions set out in it have largely been implemented.

In order to promote digital finance in Europe, while adequately regulating its risks, in light of the mission letter of Executive Vice-President Dombrovskis the Commission services are working towards a new Digital Finance Strategy for the EU. Key areas of reflection include deepening the Single Market for digital financial services, promoting a data-driven financial sector in the EU while addressing its risks and ensuring a true level playing field, making the EU financial services regulatory framework more innovation-friendly, and enhancing the digital operational resilience of the financial system.

This public consultation, and the parallel public consultation on digital operational resilience, are first steps to prepare potential initiatives which the Commission is considering in that context. The Commission may consult further on other issues in this area in the coming months.

As regards blockchain, the European Commission has a stated and confirmed policy interest in developing and promoting the uptake of this technology across the EU. Blockchain is a transformative technology along with, for example, artificial intelligence. As such, the European Commission has long promoted the exploration of its use across sectors, including the financial sector.

Crypto-assets are one of the major applications of blockchain for finance. Crypto-assets are commonly defined as a type of private assets that depend primarily on cryptography and distributed ledger technology as part of their inherent value². For the purpose of this consultation, they will be defined as "a digital asset that may depend on cryptography and exists on a distributed ledger". Thousands of crypto-assets, with different features and serving different functions, have been issued since Bitcoin was launched in 2009³. There are many ways to classify the different types of crypto

assets⁴. A basic taxonomy of crypto-assets comprises three main categories: 'payment tokens' that may serve as a means of exchange or payment, 'investment tokens' that may have profit-rights attached to it and 'utility tokens' that may enable access to a specific product or service. The crypto-asset market is also a new field where different actors – such as the wallet providers that offer the secure storage of crypto-assets, exchanges and trading platforms that facilitate the transactions between participants – play a particular role

Crypto-assets have the potential to bring significant benefits to both market participants and consumers. For instance, initial coin offerings (ICOs) and security token offerings (STOs) allow for a cheaper, less burdensome and more inclusive way of financing for small and medium-sized companies (SMEs), by streamlining capital-raising processes and enhancing competition. The 'tokenisation' of traditional financial instruments is also expected to open up opportunities for efficiency improvements across the entire trade and post-trade value chain, contributing to more efficient risk management and pricing⁵. A number of promising pilots or use cases are being developed and tested by new or incumbent market participants across the EU. Provided that platforms based on Digital Ledger Technology (DLT) prove that they have the ability to handle large volumes of transactions, it could lead to a reduction in costs in the trading area and for post-trade processes. If the adequate investor protection measures are in place, crypto-assets could also represent a new asset class for EU citizens. Payment tokens could also present opportunities in terms of cheaper, faster and more efficient payments, by limiting the number of intermediaries.

Since the publication of the FinTech Action Plan in March 2018, the Commission has been closely looking at the opportunities and challenges raised by crypto-assets. In the FinTech Action Plan, the Commission mandated the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) to assess the applicability and suitability of the existing financial services regulatory framework to crypto-assets. The advice⁶ received in January 2019 clearly pointed out that while some crypto-assets fall within the scope of EU legislation, effectively applying it to these assets is not always straightforward. Moreover, there are provisions in existing EU legislation that may inhibit the use of certain technologies, including DLT. At the same time, EBA and ESMA have pointed out that most crypto-assets are outside the scope of EU legislation and hence are not subject to provisions on consumer and investor protection and market integrity, among others. Finally, a number of Member States have recently legislated on issues related to crypto-assets which are currently not harmonised.

A relatively new subset of crypto-assets – the so-called "stablecoins" – has emerged and attracted the attention of both the public and regulators around the world. While the crypto-asset market remains modest in size and does not currently pose a threat to financial stability⁷, this may change with the advent of "stablecoins", as they seek a wide adoption by consumers by incorporating features aimed at stabilising their 'price' (the value at which consumers can exchange their coins). As underlined by a recent G7 report⁸, if those global "stablecoins" were to become accepted by large networks of customers and merchants, and hence reach global scale, they would raise additional challenges in terms of financial stability, monetary policy transmission and monetary sovereignty.

Building on the advice from the EBA and ESMA, this consultation should inform the Commission services' ongoing work on crypto-assets⁹: (i) For crypto-assets that are covered by EU rules by virtue of qualifying as financial instruments under the [Markets in financial instruments Directive – MiFID II](#) – or as electronic money/e-money under the [Electronic Money Directive – EMD2](#) – the Commission services have screened EU legislation to assess whether it can be effectively applied. For crypto-assets that are currently not covered by the EU legislation, the Commission services are considering a possible proportionate common regulatory approach at EU level to address, inter alia, potential consumer/investor protection and market integrity concerns.

Given the recent developments in the crypto-asset market, the President of the Commission, Ursula von der Leyen, has stressed the need for "a common approach with Member States on crypto-currencies to ensure we understand how to make the most of the opportunities they create and address the new risks they may pose"¹⁰. Executive Vice-president Valdis Dombrovskis has also indicated his intention to propose a new legislation for a common EU approach on crypto-assets, including "stablecoins". While acknowledging the risks they may present, the Commission and the Council have also jointly declared that they "are committed to put in place the framework that will harness the potential opportunities that some crypto-assets may offer"¹¹.

Responding to this consultation and follow up to the consultation

In this context and in line with [Better regulation principles](#), the Commission is inviting stakeholders to express their views on the best way to enable the development of a sustainable ecosystem for crypto-assets while addressing the major risks they raise. This consultation document contains four separate sections.

First, the Commission seeks the views of all EU citizens and the consultation accordingly contains a number of more general questions aimed at gaining feedback on the use or potential use of crypto-assets.

The three other parts are mostly addressed to public authorities, financial market participants as well as market participants in the crypto-asset sector:

- **The second section seeks feedback from stakeholders on whether and how to classify crypto-assets.** This section concerns both crypto-assets that fall under existing EU legislation (those that qualify as ‘financial instruments’ under MiFID II and those qualifying as ‘e-money’ under EMD2) and those that do not.
- **The third section invites views on the latter, i.e. crypto-assets that currently fall outside the scope of the EU financial services legislation. In that first section, the term ‘crypto-assets’ is used to designate all the crypto-assets that are not regulated at EU level¹². At certain point in that part, the public consultation makes further distinction among those crypto-assets and uses the terms ‘payment tokens’, “stablecoins” ‘utility tokens’, ‘investment tokens’.. The aim of these questions is to determine whether an EU regulatory framework for those crypto-assets is needed. The replies will also help identify the main risks raised by unregulated crypto-assets and specific services relating to those assets, as well as the priorities for policy actions.**
- **The fourth section seeks views of stakeholders on crypto-assets that currently fall within the scope of EU legislation, i.e. those that qualify as ‘financial instruments’ under MiFID II and those qualifying as ‘e-money’ under EMD2. In that section and for the purpose of the consultation, those regulated crypto-assets are respectively called ‘security tokens’ and ‘e-money tokens’.** Responses will allow the Commission to assess the impact of possible changes to EU legislation (such as the Prospectus Regulation , MiFID II, the Central Security Depositories Regulation, ...) on the basis of a preliminary screening and assessment carried out by the Commission services. This section is therefore narrowly framed around a number of well-defined issues related to specific pieces of EU legislation. Stakeholders are also invited to highlight any further regulatory impediments to the use of DLT in the financial services.

To facilitate the reading of this document, a glossary and definitions of the terms used is available at the end.

The outcome of this public consultation should provide a basis for concrete and coherent action, by way of a legislative action if required.

This consultation is open until 19 March 2020.

¹ [Commission's Communication: "FinTech Action Plan: For a more competitive and innovative European financial sector"](#) (March 2018)

² [EBA report with advice for the European Commission on 'crypto-assets'](#), January 2019

³ [ESMA, "Advice on initial coin offerings and Crypto-Assets"](#), January 2019;

⁴ See: ESMA Securities and Markets Stakeholder Group, Advice to ESMA, October 2018

⁵ Increased efficiencies could include, for instance, faster and cheaper cross-border transactions, an ability to trade beyond current market hours, more efficient allocation of capital (improved treasury, liquidity and collateral management), faster settlement times and reduce reconciliations required. See: Association for Financial Markets in Europe, 'Recommendations for delivering supervisory convergence on the regulation of crypto-assets in Europe', November 2019.

⁶ [ESMA, "Advice on initial coin offerings and Crypto-Assets"](#), January 2019; [EBA report with advice for the European Commission on 'crypto-assets'](#), January 2019

- Don't know / no opinion / not relevant

II. Classification of crypto-assets

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

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

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

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

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

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

- Yes
- 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.

Digital assets like scriptural money are currently accounted for in proprietary ledgers at banks/financial institutions and are already regulated with “e-money” legislation. Therefore only Crypto-assets (i.e. digital assets registered on a distributed ledger technology of some kind) should be included in this initiative as the industry is waiting to get clarity on how these “novel” instruments will be treated since they open up new opportunities (e.g. transacting without intermediaries) and challenges (e.g. AML/CTF area). Other jurisdictions in Europe/EEA (Switzerland, Lichtenstein, Malta etc.) have also done the same by reviewing “DLT registered securities” specifically and crafting suitable new regulations or tweaking/applying existing ones to accommodate them. A comparative study of various countries (see <https://www.loc.gov/law/help/cryptoassets/compsum.php>) has shown how various countries have considered differing approaches to regulating crypto assets, however there is no specific mention/analysis of mere “digital assets” representing value that are not registered on a DLT of any kind. Including them in this initiative will open up existing digital assets representing value such as IP (such as patents, copyrights), content (media like audio/video) which are not registered in DLT. Having said that, there are innovative ideas emerging around tokenizing physical assets (like real-estate and potentially any other physical asset) on the blockchain that could enable fractional ownership and completely open up new ways of financing/investing/establishing ownership of physical assets.

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.

Crypto assets registered on a public DLT where the private keys (or control of assets) are retained by an intermediary (aka custodian) and not the owner of those assets could be considered as a “deposit”. Crypto custodian licensing regime has started emerging in some EU jurisdictions already (German application deadline is March 2020) and some of these players are expected to provide deposit guarantees. Alternatively, if the crypto assets are in self-custody of the asset owner at all times but are registered in a permissioned/private DLT then the parties maintaining such a ledger could be considered as maintaining a “deposit” and potentially provide a “deposit” guarantee since they are able to control the outcome of anything that is recorded in such ledgers. In contrast, assets maintained in self-custody at all times and tracked on a public DLT should not be seen as a deposit as there is no single party or consortium maintaining the ledger, parties who are providing software interface to public blockchains should not be seen as intermediaries /custodians if they are unable to control the asset or influence the transactions being recorded on the ledger in any way.

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.

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

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.

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

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

5000 character(s) maximum

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

Crypto assets registered on a public DLT where the private keys (or control of assets) are retained by an intermediary (aka custodian) and not the owner of those assets could be considered as a “deposit”. Crypto

custodian licensing regime has started emerging in some EU jurisdictions already (German application deadline is March 2020) and some of these players are expected to provide deposit guarantees. Alternatively, if the crypto assets are in self-custody of the asset owner at all times but are registered in a permissioned/private DLT then the parties maintaining such a ledger could be considered as maintaining a “deposit” and potentially provide a “deposit” guarantee since they are able to control the outcome of anything that is recorded in such ledgers. In contrast, assets maintained in self-custody at all times and tracked on a public DLT should not be seen as a deposit as there is no single party or consortium maintaining the ledger, parties who are providing software interface to public blockchains should not be seen as intermediaries /custodians if they are unable to control the asset or influence the transactions being recorded on the ledger in any way.

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 legislation¹⁵ (A.) and on the risks presented by some service providers related to crypto-assets and the best way to mitigate them (B.). This section also raises horizontal questions concerning market integrity, Anti-Money laundering (AML) and Combatting the Financing of Terrorism (CFT), consumer /investor protection and the supervision and oversight of the crypto-assets sector (C.).

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

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

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

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

Please rate from 1 (not important at all) to 5 (very important)

										Don't know /
--	--	--	--	--	--	--	--	--	--	--------------

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

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.

Fractional ownership of an otherwise illiquid asset is another expected benefit where assets ranging from real-estate to art, wine vintage could be tokenized to fractional representation of the asset and then offered to investors. Such ownership/participation could be extended to not-for-profit purposes (e.g. governance of trusts or even community/society) which is already covered under decentralized governance. Crypto-assets could also be seen as an enabler for new economic models that encourages participants to grow new decentralized networks.

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 find all of the above use-cases of crypto-assets/DLT technology as very important and beneficial for all the players included. We strongly believe that this area should be also supported by the regulators. By the regulatory support we mean reasonable regulation which will not stifle further development.

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 manipulation¹⁶. 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 competition¹⁷. 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 stability¹⁸, this might change in the future.

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

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

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

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

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	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Market integrity (e.g. price, volume manipulation, ...)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Investor/consumer protection	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-money laundering and CFT issues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data protection issues	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Competition issues	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber security and operational risks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Taxation issues	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Energy consumption entailed in crypto-asset activities	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Financial stability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Monetary sovereignty/monetary policy transmission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

We do not see any additional risks significant enough to be further mentioned.

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.

During systemic shocks as we see currently with the COVID-19 virus, central bankers may attempt to influence the economy with policy measures. The risk with “decentralized” crypto assets (specially those which aim to be payment instruments/currencies) is that it may be harder to influence (in case they will ever be in a position of a major currency player, which is not the case at the moment) and thus is marked as higher risk in the assessment to financial stability/monetary sovereignty. They are also exposed to cyber security risks (51% attack for example) as some of the underlying infrastructure becomes concentrated in a certain geography (e.g. China). Some of the privacy centric crypto assets open up the issues around AML /CFT. Hence these are rated highest risks.

“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.

One of the major reasons for the lack of adoption of existing cryptocurrency as a payment instrument has been the high volatility. Stable coins tackle this and could finally deliver the promise of efficient low cost and fast payment using such instruments along with all the other benefits associated with cryptocurrencies (financial inclusion, transparency and traceability). While “stable coins”pegged to national/fiat currencies could provide such impact within specific countries, “global stable coins” could help increase the scale of such impact tremendously. Making international/cross-border monetary transactions highly efficient. This would have a huge benefit to the economy, especially to emerging economies where the national monetary policies are not well run and the local currencies are at constant risk of devaluation.

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	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Market integrity (e.g. price, volume manipulation...)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Investor/consumer protection	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-money laundering and CFT issues	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data protection issues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Competition issues	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber security and operational risks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Taxation issues	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Energy consumption	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Financial stability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Monetary sovereignty/monetary policy transmission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

Further risk that we see especially in connection with closed group of companies that run a private stablecoin (e.g. Libra association) is that it can easily create “concentration of power and information”, especially in the sense of collecting information about spending behaviors. With recent scandalous behavior of companies like Facebook, it is worth assessing whether the EU would like to give its monetary sovereignty to such private companies.

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.

The obvious main difference is that the “global stablecoins” will have a global reach and therefore the risks, especially in connection with power and information concentration is much higher. However, it is important to highlight that all stablecoins, due to their digital nature, have the potential to become global. We therefore do not see too much value in differentiating between “stable coins” and “global stablecoins”.

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.

We believe that without a bespoke EU financial services legislation we run the risk of different national interpretation and regulations that will make it harder to achieve a single EU market for crypto assets (also potentially making it harder to align with a global regulation that might emerge in the future). The main characteristic of all digital assets is that they are borderless, which means that if the legislation or regulation aims to be effective, it has to be done on a wide-reaching level and with common interpretation.

Question 15. What is your experience (if any) as regards national regimes on c r y p t o - a s s e t s ?

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.

In Germany, for example, from the tax point of view, crypto assets are treated as long-term capital gains which is a great incentive for people to use these assets. On the negative side of things, the custodian regulations tend to favour existing custodians (legacy financial institutions like banks) making it harder for innovative startups to flourish and come up with innovative solutions. It is generally a problem of all the European jurisdictions that they have a hard time to fit the existing legislation and legacy technological systems to the new upcoming solutions and technology. Most of the time there is a lack of legal certainty among the young progressive companies which sometimes hinder the progress of the innovative solutions. Tools like fintech innovation hubs or regulatory sandboxes would definitely help the cause. Common EU-wide approach is the ideal scenario.

Question 16. In your view, how would it be possible to ensure that a bespoke regime for crypto-assets and crypto-asset service providers is proportionate to induce innovation, while protecting users of crypto-assets?

Please indicate if such a bespoke regime should include the above-mentioned categories (payment, investment and utility tokens) or exclude some of them, given their specific features (e.g. utility tokens).

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 it is especially important to give clarity on the types/definitions of crypto-assets and clearly identify those that need to be regulated. For the ones that need to be regulated, unambiguous but technically feasible requirements for service providers should be set up, to meet such obligations in a relatively uncomplicated manner.

Also, young innovative companies with short lifespans usually need fast regulatory support, which most of the time lacks from the side of regulators/supervisors. When giving out approvals, licences, regulatory opinions, etc., the regulators should use flexible tools like regulatory sandboxes, fintech contact points, innovation hubs etc. to make sure that innovative startups are supported.

To encourage innovation, the regulation should be common for the whole EU and also flexible (i.e. not overly defensive/conservative) and give guidance on all recently known types of crypto assets.

As an example of overly defensive/conservative legislation we can give the AML law in the Czech Republic, which stated the “obliged entity” under such law is any company which does any business in relation to crypto-assets. These overly conservative catch-all clauses which tend to regulate everything are the very reason why some innovative companies cannot flourish as they are burdened by extensive legal requirements.

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

If you answered yes to question 17, please indicate how this clarity should be provided (guidance, EU legislation, ...):

5000 character(s) maximum

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

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.

While clarity on how exposure of financial institutions to crypto-assets is going to be treated will definitely help unlocking the potential of crypto assets and will allow institutional money and institutional services to enter the crypto area. Any overly conservative treatment has the tendency to stifle the new upcoming industry innovation. Currently, most of the private banks have no guidance on how to act towards crypto assets and most of the time they take a very conservative, even averse stand, which is detrimental not only to the new businesses, but also to the existing ones. There are examples when financial institutions are

closing down accounts to businesses just on the basis that the business is somehow connected to crypto assets (although it is a perfectly legal business). Such fearful behaviour of the traditional players is not acceptable if the goal is innovation.

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.

Absolutely, this would open up innovative application of this technology to bring liquidity and fractional ownership to highly illiquid assets across the EU market. Great example of a jurisdiction which already changed their civil law in the sense that it will allow for flexible creation, storage and change of ownership of crypto-assets is Liechtenstein. Please see the details of this novel legislation for example here: <https://impuls-liechtenstein.li/en/blockchain-act-liechtenstein/>

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.

We took Germany as an example with some of the following providers:

- crypto-asset issuers: Neufund, Bitbond, WeVest
- exchanges: Bison App, Boerse Stuttgart
- wallet providers: Solar, Upvest

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 consider that the sponsor or issuer of a crypto asset need not be established in the EU but it should be easy for such an entity/individuals to approach preferably a EU-wide regulator or supervisory entity (or in an absence of such entity, the access to the EU market should be feasible, for example having the option of passporting of approvals of national regulators across the EU). This is so that there is a minimum friction to crypto-based commerce globally.

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 conflicts of interest, ...):

5000 character(s) maximum

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

The disclosure should either be made by the true asset owner, i.e. the issuer or the sponsor as they know most about the characteristics of the respective asset (or an intermediary who is underwriting those assets, on the basis of an agreement for example). In any case, there should always be a party, which is responsible for the asset and the information that is given about such asset to the investors. Because the investors into these types of assets were in the past mostly retail investors, the information to be given should be short and concise, focusing on the crucial elements of the investment, i.e. especially potential risks connected to the investments must be clearly stated. Other information which describes the asset and its functions is, of course, also important, but it tends to be very technical, deterring the potential investors to read the material. Maybe it would be helpful to distinguish the information about the investment and its risks from the information about the technical nature and use-case of the given asset, not to confuse the retail investor.

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)	Don't know / no opinion / not relevant
The Consumer Rights Directive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The E-Commerce Directive	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The EU Distance Marketing of Consumer Financial Services Directive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

We are not aware of any such legislation.

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.

N/A

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	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 are of the opinion that if the above potential obligations would be applicable, it would be a great start. The market would then need to be monitored, to assess whether further requirements are necessary.

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.

We believe that the above mentioned regulatory standards should be put in place because of the following reasons:

fitness and probity standards: because of the fact that in the early days of crypto assets, there were many individuals who were repeatedly misleading the investors, it is important to establish a mechanism which will ensure that the unfair players will be eradicated from the market.

advertising rules: There were a number of cases when different crypto assets were advertised in a misleading manner, especially by anonymous online social media personas, with the intention to mislead the public and misinform about the quality of the projects and people behind them. Regulation in this area would be highly appreciated.

safeguarding of funds: There were many cases in the past, when the issuer of crypto assets stole the crowdfunded money or did not use them for the intended purpose. These safeguards are therefore very important.

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.

As mentioned above, we believe that given the digital nature of stablecoins and therefore having the ability to work borderless, all the stablecoins have the potential to become “global”. One of the distinctive factors could be the underlying asset/currency to which the stablecoin is pegged. When the coin is representing /pegged to a national currency it could be seen as a “ordinary” stablecoin (for example Tether, which is pegged 1:1 to the USD, or at least claims so). When the coin is pegged to a basket of global currencies (like it is foreseen with the Libra project), it could be seen as a “global” stablecoin, potentially positioned as a legal tender to be accepted globally. Another distinctive factor could be the actual reach of the coin (i.e. companies like Facebook can make their Libra coin “global” overnight while smaller issuers may start only with some local use-case of a coin), although we understand that such a factor would not be easily and objectively measured.

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, ...)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The assets or funds of the reserve should be segregated from the issuer’s balance sheet	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Obligation for the assets or funds to be held in custody with credit institutions in the EU	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Periodic independent auditing of the assets or funds held in the reserve	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 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, ...)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The assets or funds of the reserve should be segregated from the issuer's balance sheet	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Obligation for the assets or funds to be held in custody with credit institutions in the EU	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Obligation for the assets or funds to be held for safekeeping at the central bank	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Periodic independent auditing of the assets or funds held in the reserve	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Obligation for the issuer to use open source standards to promote competition	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

We are of the opinion that if the above requirements will be met, it will be satisfactory. I.e. no further requirements needed.

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.

All the requirements are relevant as they are ensuring the fundamentals underpinning the stability of a stable coin. We recommend to follow the case of Tether, some recent information here for example: <https://cointelegraph.com/news/proving-that-tether-manipulated-bitcoin-2017-bull-run-wont-be-easy>
This case can be a good example of what can go wrong with stablecoins. I.e. not holding enough reserve, no audits, possible manipulation of markets through “excessive printing/issuance” of a stablecoin, shady governance structure, etc.

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, ...)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The assets or funds of the reserve should be segregated from the issuer's balance sheet	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Obligation for the assets or funds to be held in custody with credit institutions in the EU	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Periodic independent auditing of the assets or funds held in the reserve	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

Same reasoning as for the “ordinary stablecoins”. We are of the opinion that if the above requirements will be met, it will be satisfactory. I.e. no further requirements needed.

25.2 b) 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.

Same reasoning as for the “ordinary stablecoins”. All the requirements are relevant as they are ensuring the fundamentals underpinning the stability of a stable coin. We recommend to follow the case of Tether, some recent information here for example: <https://cointelegraph.com/news/proving-that-tether-manipulated-bitcoin-2017-bull-run-wont-be-easy>

This case can be a good example of what can go wrong with stablecoins. I.e. not holding enough reserve, no audits, possible manipulation of markets through “excessive printing/issuance” of a stablecoin, shady governance structure, etc.

“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.

Based on the recent Bank of International Settlements report: <https://www.bis.org/publ/bppdf/bisap107.pdf>, around 80 per cent of central banks worldwide are working on issuance of CBDCs (central bank digital currencies). It is questionable whether something like a “wholesale stablecoin” will be needed in the case that CBDCs will be in place. It can be expected that CBDCs will have their own set of rules as being “public” money as opposed to “privately” issued stablecoins. (by the way, some of the private stablecoins may also lose their use-case when CBDCs will come into play, there will be no use-case for Tether for example, if an USD CBDC will come into play)

If we look at stablecoins only, leaving CBDCs aside, then we believe that the rules should be the same no matter which entity is issuing them. The opportunity now is to adopt a new flexible payment instrument with low fees for cross-border payments, especially for the retail sector. If banks need to develop some sort of internal tokens for their settlement operations, then such a solution should not probably be seen as a stablecoin, but rather a token for an internal settlement system. But, of course, such a token then could not leave the internal (private) network, i.e. could not be used outside such a system by other entities. If banks would try to develop a stablecoin which would have value also for other entities, then such stablecoin must adhere to the same regulation as any other stablecoins.

2. Trading platforms

Trading platforms function as a market place bringing together different crypto-asset users that are either looking to buy or sell crypto-assets. Trading platforms match buyers and sellers directly or through an intermediary. The business model, the range of services offered and the level of sophistication vary across platforms. Some platforms, so-called 'centralised platforms', hold crypto-assets on behalf of their clients while others, so-called decentralised platforms, do not. Another important distinction between centralised and decentralised platforms is that trade settlement typically occurs on the books of the platform (off-chain) in the case of centralised platforms, while it occurs on DLT for decentralised platforms (on-chain). Some platforms have already adopted good practice from traditional securities trading venues¹⁹ while others use simple and inexpensive technology.

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

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

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	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of adequate governance arrangements, including operational resilience and ICT security	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Absence or inadequate segregation of assets held on the behalf of clients (e.g. for 'centralised platforms')	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Conflicts of interest arising from other activities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Absence/inadequate recordkeeping of transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Absence/inadequate complaints or redress procedures are in place	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Bankruptcy of the trading platform	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lacks of resources to effectively conduct its activities	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Losses of users' crypto-assets through theft or hacking (cyber risks)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of procedures to ensure fair and orderly trading	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Access to the trading platform is not provided in an undiscriminating way	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Delays in the processing of transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
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)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

Main risks in crypto trading venues are concentrated at and dominated by licensed centralized platforms (the fact that these platforms are centralized also leads to other issues like discriminatory access, anti-competitive behaviour or honeypots for hackers, etc.). Other main risks of centralized trading platforms include lack of transparency about services offered, and sometimes also fee structure, and available APIs. We, therefore, believe that decentralized exchanges (DEXes) should be encouraged, and any necessary regulatory requirements (like investor protection, anti-fraud requirements, etc.) should be clarified to the developers of such platforms so it can be well addressed.

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.

As any business offered to the public, trading platforms (centralised or decentralised) should have clear available service description, in an easy to read (acceptable) language. The provision of services, access (including API documentation and access) and the fees should be clearly stated and properly documented.

We believe decentralised exchanges are the future, mainly because it can save costs (because of less intermediation), provide for lower fees and provide easy access to investments/trading to the general public.

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)	Don't know / no opinion / not relevant
Trading platforms should have a physical presence in the EU	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trading platforms should segregate the assets of users from those held on own account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Trading platforms should be subject to rules on conflicts of interest	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Trading platforms should be required to keep appropriate records of users' transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Trading platforms should have an adequate complaints handling and redress procedures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Trading platforms should be subject to prudential requirements (including capital requirements)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trading platforms should have adequate rules to ensure fair and orderly trading	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trading platforms should provide access to its services in an undiscriminating way	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trading platforms should be responsible for screening crypto-assets against the risk of fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 platforms should publish openly their rules of operation, including fee structures and other hidden costs, as well as documentation on available services and APIs, client eligibility and general trading rules, including non-compliance measures.

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.

We are of the opinion that if the traded crypto assets are of small capitalisation or have services value (utility - e.g. Ether) rather than security or payment function (e.g. Bitcoin), such crypto assets do not require overly strict supervision and do not have to be subject to the same reporting, and screening requirements.

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

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.

Lack of transparency about service offer, fee structure and available APIs. Other risk factors involve general accountability, transparency about the business, the ultimate beneficiaries of the business and governance in place.

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.

All risks associated with trading platforms and/or exchanges are no more or less than those for any other business. Fraud is unacceptable and proper IT systems in place are in every market player's own interest. There is no point in regulating IT systems, because of constant technological evolution therein. A fixed set of requirements will only guarantee a failure of systems and businesses will be thwarted in their normal development progression. The motivation for exchange business should be to stay in business for as long as possible, employing the best general business practices.

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	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exchanges should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exchanges should segregate the assets of users from those held on own account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Exchanges should be subject to rules on conflicts of interest	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Exchanges should be required to keep appropriate records of users' transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Exchanges should have an adequate complaints handling and redress procedures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Exchanges should be subject to prudential requirements (including capital requirements)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Exchanges should be subject to advertising rules to avoid misleading marketing/promotions	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exchanges should be responsible for screening crypto-assets against the risk of fraud	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

Exchanges should publish openly their rules of operation, including fee structures and other hidden costs, as well as documentation on available services and APIs, client eligibility and general trading rules, including non-compliance measures.

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.

We are of the opinion that if the traded crypto assets are of small capitalisation or have services value (utility - e.g. Ether) rather than security or payment function (e.g. Bitcoin), such crypto assets do not require overly strict supervision and do not have to be subject to the same reporting, and screening requirements.

4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys²⁰ 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 specific²¹. DLT networks generally provide their own wallet functions (e.g. Bitcoin or Ether).

There are also specialised wallet providers. Some wallet providers, so-called custodial wallet providers, not only provide wallets to their clients but also hold their crypto-assets (i.e. their private keys) on their behalf. They can also provide an overview of the customers' transactions. Different risks can arise from the provision of such a service.

²⁰ DLT is built upon a cryptography system that uses pairs of keys: public keys, which are publicly known and essential for identification, and private keys, which are kept secret and are used for authentication and encryption.

²¹ There are software/hardware wallets and so-called cold/hot wallets. A software wallet is an application that may be installed locally (on a computer or a smart phone) or run in the cloud. A hardware wallet is a physical device, such as a USB key. Hot wallets are connected to the internet while cold wallets are not.

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

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	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of adequate governance arrangements, including operational resilience and ICT security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Absence or inadequate segregation of assets held on the behalf of clients	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Conflicts of interest arising from other activities (trading, exchange)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Absence/inadequate recordkeeping of holdings and transactions made on behalf of users	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Absence/inadequate complaints or redress procedures are in place	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bankruptcy of the custodial wallet provider	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Inadequate own funds to repay the consumers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The custodial wallet is compromised or fails to provide expected functionality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The custodial wallet provider behaves negligently or fraudulently	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

No contractual binding terms and provisions with the user who holds the wallet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------	-----------------------	----------------------------------	-----------------------	-----------------------

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.

We are not aware of any other specific risks in connection with custodial wallets. These service providers should have the same level of responsibility towards their users as any other business.

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.

Custodial wallet providers are the backbone of the security when dealing with the crypto assets. It should be ensured that these providers comply with the highest available technological and legal standards.

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	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Custodial wallet providers should be subject to governance arrangements (e.g.						

in terms of operational resilience and ICT security)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Custodial wallet providers should segregate the asset of users from those held on own account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Custodial wallet providers should be subject to rules on conflicts of interest	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Custodial wallet providers should be required to keep appropriate records of users' holdings and transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Custodial wallet providers should have an adequate complaints handling and redress procedures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Custodial wallet providers should be subject to capital requirements	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Custodial wallet providers should be subject to certain minimum conditions for their contractual relationship with the consumers/investors	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

We see the above mentioned requirements as adequate.

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.

There could be a difference in requirements where there will be a difference in the technology used or the type of asset kept.

Technology: Depending on whether a public or private blockchain or even different blockchain types within the specific category is used for a particular asset, the requirements for record keeping may be different, as the record keeping may be done automatically and possibly via slightly different means via the respective blockchain technology. So the requirements may change but the standards should be the same.

Type of an asset: In the future, the wallet providers which will deal with security tokens will need to have additional responsibilities when it comes to tracking of the ownership of the underlying real asset. i.e. they will possibly be the ones who will need to ensure the parity between the digital ownership and the real world ownership of an asset.

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 have access to the crypto assets directly by holding the private keys of the asset owner themselves (or indirectly by having permissions to control the asset in some way), there should be ideally be single set of clear regulations to comply to irrespective of the type of the token (utility vs security). Although the security tokens will most likely need some additional regulation, it should be done in a way which there will be a single set of rules for all the crypto assets plus additional for more regulatory difficult assets, such as security tokens. This will ensure for minimal bureaucracy and a single approval/authorization process. The custodial wallet provider may then have the opportunity to choose to start with only payment /utility tokens first and should it decide later to also include security tokens, it will only build on to the existing requirements additional requirements, which will be extra for e.g. security tokens.

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.

Custodial wallet providers who are also acting as broker-dealers in marketing crypto assets to retail investors should be compliant with appropriate regulations. Custodial wallet providers shouldn't be allowed to do centralized trading to avoid conflict of interest and market manipulation risks. However, non-custodial wallet providers could be allowed to connect centralized/de-centralized exchanges for trading.

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Execution of orders on crypto-assets on behalf of clients	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Crypto-assets portfolio management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Advice on the acquisition of crypto-assets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Underwriting of crypto-assets on a firm commitment basis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Placing crypto-assets on a firm commitment basis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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

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.

Not to our knowledge.

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.

The services that we have left unregulated or with lower regulation level are mining services, developers services and information services. We do not believe that the current rules could be applicable to these services, because of the technological differences from the services typically covered by MiFID II.

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

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

- 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.

Because PSD2 only aims at FIAT money and electronic money (which is a digital representation of FIAT money) and puts in place comprehensive rules for payment services with respect to such money, it should not be applicable to crypto-assets. When speaking about crypto-assets in this regard, we mean payment tokens, such as bitcoin, etc. The reason is because different payment tokens have different ways to make payments safe - some of them allow even for anonymous payments. They work on a different technology as well, so the rules of PSD2 could not be applicable, because the technology (typically blockchain) allows for different types of security of payments than PSD2.

C. Horizontal questions

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

1. Market Integrity

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

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Volume manipulation (wash trades...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Pump and dump schemes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Manipulation on basis of quoting and cancellations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dissemination of misleading information by the crypto-asset issuer or any other market participants	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Insider dealings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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.

Any risks that are historically connected to trading of traditional assets are applicable here as well.

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.

In the past, most of the above listed fraudulent behaviours were the reality of the unregulated crypto exchanges. Nevertheless, because of the growing competition between the exchanges, many started to self-regulate themselves to attract new customers. This is an on-going trend. We believe, however, that EU-wide minimal common standards should be implemented in order to ensure the trustworthiness of the crypto asset market. The solution may be to simply develop a single standard that may take inspiration from the national regulations of entities on regulated markets, which was implemented for example in Italy during the year 2019.

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

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

5000 character(s) maximum

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

We believe that common minimal standards should be developed and the inspiration may be taken from the traditional markets.

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

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.

This requirement should possibly be in place for trades above certain thresholds. However, we don't believe that it should be a general requirement, given the decentralized nature of some of the exchanges.

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.

We are of the opinion that this will be very hard to ensure given the nature of the technology behind these assets and decentralized nature of some of the exchange/trading tools.

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.

We strongly believe that harmonization of the basic definitions which will also further clarify the regulations which will follow, is always the preferred way, because the space for legal uncertainty will be significantly reduced and the development of the innovative businesses will then be more easily facilitated.

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

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

- Yes
- No
- Don’t know / no opinion / not relevant

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 are of the opinion that no further crypto asset businesses should be put under the regulation of EU AML /CTF framework as this current setup already covers the main gate-keepers who allow for the entrance to the crypto asset space from the FIAT currency space. Further regulation in this area would most likely have a detrimental effect on the innovative crypto asset businesses.

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.

Same reasoning as under question 42 above is applicable here.

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.

We do not hold any specific view in this regard.

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 do not hold any specific view in this regard. However, we are of the opinion that the current EU AML /CTF standards are satisfactory.

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
Directors and senior management of such providers should be subject to fit and proper test from a money laundering point of view, meaning that they should not have any convictions or suspicions on money laundering and related offences	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Service providers must be able to demonstrate their ability to have all the controls in place in order to be able to comply with their obligations under the anti-money laundering framework	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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.

We believe that personal responsibility and operational safeguards are indeed important factors to facilitate for trustworthy services in this area.

3. Consumer/investor protection²¹

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 investors²². Offerings of utility tokens, for instance, do not provide for minimum investment amounts nor are they necessarily limited to professional or sophisticated investors. When considering the consumer protection, the functions of the crypto-assets should also be taken into consideration. While some crypto-assets are bought for investment purposes, other are used as a means of payment or for accessing a specific product or service. Beyond the information that is usually provided by crypto-asset issuer or sponsors in their 'white papers', the question arises whether providers

of services related to crypto-assets should carry out suitability checks depending on the riskiness of a crypto-asset (e.g. volatility, conversion risks, ...) relative to a consumer's risk appetite. Other approaches to protect consumers and investors could also include, among others, limits on maximum investable amounts by EU consumers or warnings on the risks posed by crypto-assets.

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

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

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

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')	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Limits on the investable amounts in crypto-assets by EU consumers	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Suitability checks by the crypto-asset service providers (including exchanges, wallet providers, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Warnings on the risks by the crypto-asset service providers (including exchanges, platforms, custodial wallet providers, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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 believe that above consumer protection measures are adequate as the most important is to provide the consumers with relevant information and quantify the risk connected to their potential investment.

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.

It is important to ensure an informed investment, and to provide the consumers with a set of minimum mandatory information concerning both the performance of the platform itself and the risks to which investors are exposed. The same logic must be applied to all the crypto assets which function is to offer an alternative investment tool. Therefore, we believe that similar standards should be applied to all crypto assets which have primarily investment function.

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.

When it comes to payment tokens or utility tokens, it can be argued that the consumer is already quite well informed about the function of such a token and can assess the risk in connection with it. For utility tokens, the buyer must know that he/she is buying the token to specifically use it on the respective platform to get some service - in this case it is not relevant to inform him about his investment risks as the reason to buy the token is not to invest but rather use a service. Same logic may be applied to payment tokens, where the utility lies in the payment service of such a token. Here again, the primary motivation of a buyer is not an investment, so information about some investment risk may be irrelevant - but of course, the consumer should be always informed about the nature of the token and about the specific risks that come with it (payment tokens may lose its value for example).

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.

Provided that private sales will be given to institutional or qualified investors only, the level of standard may be changed on that basis, i.e. such investors will most likely do their own due diligence on the asset and do not need the same risk information standard as the retail investors.

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.

Because the air dropped crypto assets are provided for free, there is no investment risk which the consumer should be aware of. The consumer should be still informed about other risks which may be connected to such assets (i.e. technological risks, etc.).

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	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Those crypto-assets should be still accessible to EU consumers/investors	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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.

We do not see any other option.

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.

Given the decentralized nature of the crypto assets it would be futile to try to ban crypto assets which do not comply with the EU standards. However, we strongly believe that the consumers should be always informed and aware that certain assets are not in compliance with EU standards. We are of the opinion that a list of crypto assets that comply with EU rules, held by a EU regulatory/supervisory entity would be appreciated by the public.

4. Supervision and oversight of crypto-assets service providers

As a preliminary remark, it should be noted that where a crypto-asset arrangement, including “stablecoin” arrangements qualify as payment systems and/or scheme, the [Eurosystem oversight frameworks may apply](#). In accordance with its mandate, the Eurosystem is looking to apply its oversight framework to innovative projects. As the payment landscape continues to evolve, the Eurosystem oversight frameworks for payments instruments, schemes and arrangements are currently reviewed with a view to closing any gaps that innovative solutions might create by applying a holistic, agile and functional approach. The European Central Bank and Eurosystem will do so in cooperation with other relevant European authorities. Furthermore, the Eurosystem supports the creation of cooperative oversight frameworks whenever a payment arrangement is relevant to multiple jurisdictions.

That being said, if a legislation on crypto-assets service providers at EU level is needed, a question arises on which supervisory authorities in the EU should ensure compliance with that regulation, including the licensing of those entities. As the size of the crypto-asset market is still small and does not at this juncture raise financial stability issues, the supervision of the service providers (that are still a nascent industry) by national competent authorities would be justified. At the same time, as some new initiatives (such as the “global stablecoin”) through their global reach and can raise financial stability concerns at EU level, and as crypto-assets will be accessible through the internet to all consumers, investors and firms across the EU, it could be sensible to ensure an equally EU-wide supervisory perspective. This could be achieved, *inter alia*, by empowering the European Authorities (e.g. in cooperation with the European System of Central Banks) to supervise and oversee crypto-asset service providers. In any case, as the crypto-asset market rely on new technologies, EU regulators could face new challenges and require new supervisory and monitoring tools.

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

5000 character(s) maximum

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

Exchanges and trading venues should possibly be subject to supervisory coordination as these providers are the main player on the crypto asset market. These market players are also normally under supervision in jurisdictions outside the EU. Also, because most of the fraudulent activity was connected with these types of entities in the past, supervision would be welcomed by the retail investors/consumers to enhance trustworthiness.

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 technological solution could possibly be some mandatory APIs to be set up by the respective trading venue/exchange through which the supervisors could track in an automated way the activity on the respective trading venue/exchange.

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 venue²³ 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 1²⁴) on trading, post-trading and other financial services concerning security tokens, such as asset management, the purpose of this part of the consultation is to seek stakeholders’ views on the issues identified below that are relevant for the application of the existing regulatory framework to security tokens.

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

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

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

Current trends concerning security tokens

For the purpose of the consultation, we consider the instances where security tokens would be admitted to trading or traded on a trading venue within the meaning of MiFID. So far, however, there is evidence of only a few instances of security tokens issuance²⁵, with none of them having been admitted to trading or traded on a trading venue nor admitted in a CSD book-entry system²⁶.

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 platforms²⁷. 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-peer²⁸ 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 platforms²⁹ are still in their infancy, with uncertain prospects for future applications in financial services due to their higher trade latency and lower liquidity. Permissionless decentralised platforms could potentially develop only at a longer time horizon when further maturing of the technology would provide solutions for a more efficient trading architecture. Therefore, it could be premature at this point in time to make any structural changes to the EU regulatory framework.

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

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

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

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

²⁶ See section IV.2.5 for further information

²⁷ Type of crypto-asset trading platforms that holds crypto-assets on behalf of its clients. The trade settlement usually takes place in the books of the platforms, i.e. off-chain.

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

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

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

5000 character(s) maximum

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

Here you can find a research on existing real security token issuances in the EU economic area: <https://www.fintelum.com/resources/tokenised/>

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.

For the purposes of clarity, we are discussing only public DLT technology, not private blockchains in this question.

For utility tokens, DLT technology has undoubtedly enabled a host of innovation in terms of fundraising, transactions and record keeping.

For security tokens, DLT cannot serve in the most efficient way at the moment, due to regulatory uncertainty and/or requirements intended for investor protection. One of the benefits however relates to fractional ownership of securities: where a specific asset may be safely divided into smaller parts by virtue of digital divisibility and transaction irreversibility. As such, these fractions of an asset or fractions of a token can be swapped between whitelisted (permitted) persons thus facilitating liquidity in potentially otherwise illiquid assets.

Even if the central (transfer) agent oversees the transactions, the process and subsequent record keeping can be effected via an automated smart contract execution on blockchain, or internally on service provider's books.

Last, but not least, the DLT technology provides certain transparency of an asset that is represented (floated) as a token on a public blockchain.

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 are of the opinion that the use of DLT technology rather offers additional advantages as stated under question 55.

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.

We do not necessarily believe that DLT will significantly impact the role and operation of the existing trading venues, but it will rather offer more options to smaller capital trading and transform trading venues for the better, i.e., more accessible to retail investors. As of now, it is mostly impossible for security tokens of any shape or size be easily traded on the secondary market. The access is restricted to MTF or OTF license holders, where retail investors are barred due to high entry barriers.

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.

We believe it would be beneficial for all market participants to first reach a consensus on basic definitions, such as difference between public and private blockchains; money, its functions and available types; different types of digital assets and tokens and then gradually come up with more detailed regulation. On the other hand EU has made groundbreaking regulatory work globally in the area of data privacy (GDPR), so possible there is an opportunity to do so also in the area of crypto/security tokens to drive innovation based on a technology that aims to drive financial inclusion. It can be the case that doing a piece-meal “gradual” approach would deliver “too little too late”. However, whatever the approach will be, the ambition should always be to deliver an appropriate set of EU wide regulations for enabling a “single digital market for digital assets”.

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.

The regulatory uncertainty is a big hindrance of the development of the security token market and potential novel funding mechanisms that can come with it. Moreover, in different EU jurisdictions, NCAs will have different approaches, it will create an inequality between the EU member states and the companies which

would like to use security tokens will be forced to do a “forum shopping” of the security token friendliest jurisdictions. It would also cause an uncertainty on the side of investors, as they may not appreciate certain rules or weak protections in certain jurisdictions. It can also be the case that because the security token issuance will be in a different country than the residence of investors, the investors may not receive the appropriate information about the security token issuance or characteristic and/or other regulatory support.

Therefore, in some cases classification differences in different member states may be a hurdle, but in the vast majority of situations security tokens will represent either equity or debt, and should, therefore, be treated as financial instruments.

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide a definition of a security token at EU level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

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.

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Hybrid tokens should qualify as unregulated crypto-assets (i.e. like those considered in section III. of the public consultation document)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The assessment should be done on a case-by-case basis (with guidance at EU level)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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.

We have contradictory opinions within our community with respect to the hybrid token cases:

The first opinion is based on the notion of legal certainty - on that basis it can be argued that if the token has any investment-type feature, it should always be considered a security token. Otherwise, the market will

always try to create some “hybridity” which would try to cover the investment feature and use rules which would be less protective to the investors, and more flexible for the issuers. The legal certainty will suffer in this scenario and there will be a lot of pressure on the regulators to deal with the case-by-case approach, which will most likely create a lot of confusion and uncertainty.

On the other hand, the second opinion of our members encourages innovation, even if it comes at the expense of bending the status quo and of existing rules (which should, therefore, become more flexible). Hybrid tokens in this scenario should be considered on a case-by-case basis to make sure, that the innovative approaches of some of the projects will not be suppressed by too rigid legislation.

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.

Ad 1. above: The reasoning comes from the presumption of “legal certainty” which some of the members feel is the most important factor in this area.

Ad 2. above: Innovation typically comes about without any prior law being in place permitting it. Leaving some freedom to interpretation should be favoured as an approach to allow for flexibility and common sense.

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.

We believe that the majority of the investment services as laid down by MiFID II are applicable also to security tokens. What should not apply are rules relating to OTFs and MTFs which should most likely be drafted differently for DLT technology based exchanges, such as, for example, so called decentralized exchanges (DEXes).

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
- 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.

Legal certainty on the market in this area is missing. Any kind of clarification or guidance would be very welcomed.

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.

Security tokens are investment instruments like any other, so any services of investment firms in that connection should be applicable to security tokens as well. However, because security tokens may provide for more flexible trading because of the use of DLT technology (example DEXes) or creation of assets fractions, it should be made sure, that the regulation does not stall the opportunity of trading done by individuals (or so called retail investors) through these novel ways of trading.

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.

1.4. Trading venues

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

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

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

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

a d d r e s s e d ?
Please explain your reasoning.

5000 character(s) maximum

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

Decentralized exchanges (DEXes) should be considered and allowed. Examples of jurisdictions that in some way allowed for such trading venues are Liechtenstein or Switzerland.

At its core, these exchanges are non-custodial peer-to-peer exchanges for security tokens and STOs (security token offerings, i.e. new listings of security tokens) built on some public blockchain like Ethereum or Stellar. It is designed to facilitate automatic digital asset exchange between different tokens/crypto-assets. Unlike centralized exchanges that maintain an order book to match buyers and sellers, these solutions may use liquidity reserves to facilitate the exchange of digital assets, eliminating the centralized order book. All trades happen directly on-chain.

Some of these exchanges charge no listing fees, no trading fees, and no investor onboarding fees. Thus allowing for an efficient trading venue which anyone can join and access the investment opportunities without unnecessary intermediaries.

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, possible additions regarding explanations of the technical characteristics of security tokens, and possible additional risks (mainly technological) connected with security tokens should be considered.

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.

Yes, social media played a major role during the 2017-2018 crypto frenzy and many scammers and/or unfair online traders or digital asset issuers used these channels to trick the public into buying specific tokens or other digital assets. It should be made clear what is allowed on social media and what is not, to deter unfair players from miscommunication, misinformation, misleading of the public and other potentially illegal activities.

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.

The protection of investors is one of the crucial aspects of taking the DLT technology and security tokens to the mainstream as it will strengthen the confidence of the general public in these new investment instruments. We see no particular issues with applying the MiFID investor protection standards to security tokens and we also see that some of the current players in the security token sector are developing their own investor protection mechanisms (provision of adequate information to investors, enhanced transparency, etc.) to assure (more) safety of the respective investments. This proves that there is real demand on the security token market for these protections and assurances.

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.

Yes, we believe that for SME Growth Markets especially, the DLT technology can bring several advantages. One of the main advantages is the possibility of access to investments/trading by the general public, retail investors, i.e. the so called “crowd”. Many countries all around the world still have considerable obstacles to investments for retail investors. One of the possible ways for them to invest in innovative young companies is crowdfunding. But crowdfunding platforms rarely provide for secondary market options, with the possibility to exit the investments. DLT and crypto-assets are the perfect tool to provide for flexible investments/trading. Some of the main advantages include lower cost of listing, creation of digital fractions of underlying “real assets” and therefore higher affordability and lower risk for smaller investors, lower transaction fees (because DLT-based platforms may be created without unnecessary intermediaries), and bigger flexibility (it is simple to join and operate on DLT-based platforms compared to more traditional venues, may be done through very user friendly web applications or even mobile).

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 access³⁰ shall have in place effective systems procedures and arrangements to ensure that members are only permitted to provide such services if they are investment firms authorised under MiFID II or credit institutions. The same requirements also apply to MTFs and OTFs according to Article 18(5). These requirements could be an issue for security tokens, considering that crypto-asset trading platforms typically provide direct access to retail investors.

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

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

5000 character(s) maximum

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

The main advantage of security tokens is that it should have more flexibility (ease of use) in the sense of digital trading and also that it will be more accessible to the general public (lower costs and fees). To restrict the access to these financial instruments to investment firms only will only cause that these instruments will not be used and people will still tend to create other types of tokens with better access (such as payment tokens, utility tokens, etc.)

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.

We believe that having basic rules which would make clear trading criteria of security tokens, taking into account their digital nature and technology behind them, would be very useful in order to bring these assets to the mainstream.

Question 1.9 Access to a trading venues

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

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

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 direct access to trading venues to a broader base of clients, i.e. retail clients, general public or the so-called "crowd" may bring the following risks and benefits:

Risks:

Possible risks may exist in connection with the lack of experience of retail investors with trading (lack of understanding of the functionalities of the trading venue, trading tools, trading strategies, etc.) Nevertheless, this may be mitigated by clear explanations and provision of adequate information by the respective trading venue.

Benefits:

- access of general public to trading/investment opportunities with low costs and fees
- will create better financial literacy among the general public
- these trading venues will have the possibility to be accessed from anywhere, i.e. crowd from all over the world may access also global investment opportunities
- will take security tokens and other asset digitization to the mainstream - this is important also in the light of proposed CBDCs (central bank digital currencies), CBDCs will further strengthen the need to access digitized assets by public via digital means (trading venues)
- retail investors will move from riskier assets (payment tokens, utility tokens) to more traditional assets (i.e. digitized securities, other “real world” assets in the tokenized form)

1.10 Pre and post-transparency requirements

In its Articles 3 to 11, MiFIR sets out transparency requirements for trading venues in relations to both equity and non-equity instruments. In a nutshell for equity instruments, it establishes pre-trade transparency requirements with certain waivers subject to restrictions (i.e. double volume cap) as well as post-trade transparency requirements with authorised deferred publication. Similar structure is replicated for non-equity instruments. These provisions would apply to security tokens. The availability of data could perhaps be an issue for best execution³¹ of security tokens platforms. For the transparency requirements, it could perhaps be more difficult to establish meaningful transparency thresholds according to the calibration specified in MIFID, which is based on EU wide transaction data. However, under current circumstances, it seems difficult to clearly determine the need for any possible adaptations of existing rules due to the lack of actual trading of security tokens.

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

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

- 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.

In our opinion, there should not be too much of a difference between the traditional assets and digitized assets when it comes to transparency requirements. What should be kept in mind is only the different form of the security tokens and the technological possibilities of the DLT technology behind them - which should be used to have the trading capabilities more decentralized, flexible and automated. Such automation and other technological advantages may also be the groundwork for novel ways how to track the transparency requirements. In this light it is questionable whether it would make sense to mix together the traditional assets and traditional platforms with security tokens/other digital assets and security tokens trading platforms. It can be the case that these cannot be effectively mixed together on one platform, because it would have different technological bases and also different ways to deal with the transparency requirements.

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.

We do not see any particular issues with the requirements to be applied to security tokens but they must be applied in a way which is compatible with the usage of the DLT technology. We believe that further automation will also make easier (possibly also further automate) the monitoring of the transparency requirements. In this sense the regulatory approach must allow for advantageous usage of the DLT and other technology and express the requirements in a way which may be easily translated to better technological solutions which will allow not just for better trading experience but also for better (automatized) monitoring options.

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 are of the opinion that these rules should be as similar as possible also for security tokens and we do not see any particular issues why these requirements could not be used for security tokens as well. With respect to ISIN, there are already some existing crypto assets that have registered ISIN codes, thus making these assets closer to the mainstream. For example, the Association of National Number Agencies has put together a taskforce that will be labeling digital assets in an attempt to provide more clarity to investors.

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.

Yes, we believe that the respective applicable MAR provisions are appropriate to cover all cases of insider dealing for security tokens, especially given the fact that it contains the catch-all clause. We do not think that it is possible to in advance list all the possible cases of insider dealing with digital assets and therefore the practices on the market should be monitored in order to further specify the insider dealing scope in the future.

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.

Yes, we believe that the notion of market manipulation as defined by MAR is sufficiently wide with respect to security tokens. However, there were instances that certain players in the cryptocurrency market (especially the crypto exchanges, social media influencers, etc.) were suspected to manipulate the market, which can have an effect on (the price of) security tokens as well. This applies to the next question.

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.

Yes, there is a risk that the price of crypto assets will be manipulated and this will have a direct effect on the price of the security tokens. The example is the Ethereum network and its token Ether. It can be expected that the majority of security tokens will be deployed on the Ethereum network, this process is already happening. Since Ether is not considered a security token, but rather an utility token, it will fall outside the scope of MAR. It is proven by the past that when the underlying asset (i.e. Ether) is falling on price, the connected assets (such as different tokens deployed on the Ethereum network - BAT for example) tend to

fall on the price as well. This can be expected to happen in connection with security tokens deployed on the Ethereum network as well. When there is not trust of the traders/investors in the underlying technology, it will have an effect on the tokens which are deployed on the basis of that technology.

3. Short Selling Regulation (SSR)

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

According to [ESMA's advice](#), 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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Restrictions on uncovered short selling	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Competent authorities' power to apply temporary restrictions to short selling	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

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.

We are not aware of any issue that would prevent effectively applying SSR to security tokens.

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.

N/A

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 have not detected any sort of such situation.

4. Prospectus Regulation (PR)

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

4.1. Scope and exemptions

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

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

- Completely 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 believe that there should be no additional exceptions other than those which are necessary due to the different form (i.e. digital form) of the security tokens.

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 If you do agree that Delegated Regulation (EU) 2019/980 should include specific schedules about security tokens, please indicate the most effective approach: a 'building block approach' (i.e. additional information about the issuer and/or security tokens to be added as a complement to existing schedules) or a 'full prospectus approach' (i.e. completely new prospectus schedules for security tokens). Please explain your reasoning.

5000 character(s) maximum

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

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.

No. We do not identify any issues. From what we see on the market, this process has already started.

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 have not identified any difficulties of this sort.

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

- 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.

Because the typical investors into crypto assets will most likely be retail investors, it would be helpful if the prospectus regime would be simplified to provide for shorter and possibly more concise information. The typical investors into the crypto assets in the past were content with simple “white papers”. Although this documentation was not by far sufficient, it proved that retail investors are keen to have rather short and concise information available to evaluate their investment risk.

From the issuer point of view, because the security tokens will most likely be used by young companies first, regulation should be aimed at making it simpler and less expensive for such companies, to be able to access and raise money in the capital markets. The regulation should address increasing criticism that the current full regime imposes significant costs and administrative burdens on companies, seeking to raise funds publicly. To help the new digital assets thrive, it should be made sure that the regime is not too complicated or burdensome, but rather clear, straight-forward and easy to use.

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 If you do agree that issuers of security tokens should disclose specific risk factors relating to the use of DLT, please indicate if ESMA's guidelines on risks factors should be amended accordingly. Please explain your reasoning:

5000 character(s) maximum

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

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Definition of 'securities settlement system' and whether a DLT platform can be qualified as securities settlement system under the SFD	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
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;	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Definition of 'book-entry form' and 'dematerialised form	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
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);	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
What could constitute delivery versus payment in a DLT network, considering that the cash leg is not processed in the network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
What entity could qualify as a settlement internaliser	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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.

We do not see any other particular issue in this regard.

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.

In general, we believe that it will be very difficult to subsume the DLT-based settlement mechanism under the existing traditional regulation which comes from a completely different technological background. We believe that it is worth considering whether new regulation, which can be based on the regulation for traditional technology, should be drafted for a DLT-based environment, taking into consideration the advantages of the new technology.

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.

As mentioned under the question above, we believe that the regulation should be completely revamped while taking into consideration the decentralized nature of the DLT technology.

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 are not aware of any such impediments.

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on measures to prevent settlement fails	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Organisational requirements for CSDs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on outsourcing of services or activities to a third party	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on communication procedures with market participants and other market infrastructures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on the protection of securities of participants and those of their clients	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules regarding the integrity of the issue and appropriate reconciliation measures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on cash settlement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on requirements for participation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on requirements for CSD links	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on access between CSDs and access between a CSD and another market infrastructure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

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.

We do not have any strong opinions on the legal technicalities in this area.

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.

N/A

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.

We are not aware of any such additional requirements.

6. Settlement Finality Directive (SFD)

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

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

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Definition of system operator	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Definition of participant	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Definition of institution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Definition of transfer order	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
What could constitute a settlement account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
What could constitute collateral security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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 do not have any other strong opinions in this area.

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.

In general, we believe that it will be very difficult to subsume the DLT-based settlement mechanism under the existing traditional regulation which comes from a completely different technological background. We believe that it is worth considering whether new regulation, which can be based on the regulation for traditional technology, should be drafted for a DLT-based environment, taking into consideration the advantages of the new technology.

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.

Yes, we believe that such clarification would need to be in place, especially in the case of the public DLT networks. This possibly is not so much of an issue in the case of private DLT networks, where there is only a limited number of participants.

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.

N/A

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 If you do agree that the effective functioning and/or use of DLT solution is limited or constrained by any of the SFD provisions, please provide specific examples (e.g. provisions national legislation transposing or implementing SFD, supervisory practices, interpretation, application,...). Please explain your reasoning.

5000 character(s) maximum

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

7. Financial Collateral Directive (FCD)

The [Financial Collateral Directive](#) aims to create a clear uniform EU legal framework for the use of securities, cash and credit claims as collateral in financial transactions. Financial collateral is the property provided by a borrower to a lender to minimise the risk of financial loss to the lender if the borrower fails to meet their financial obligations to the lender. DLT can present some challenges as regards the application of FCD. For instance, collateral that is provided without title transfer, i.e. pledge or other form of security financial collateral as defined in the FCD, needs to be enforceable in a distributed ledger³².

³² ECB Advisory Group on market infrastructures for securities and collateral, "the potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration" (2017).

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	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If crypto-assets qualify as book-entry securities collateral	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
If records on a DLT qualify as relevant account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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 do not see any other particular issues in this area.

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.

There needs to be a clear guidance on definitions under FCD, which should be based on the harmonised definition of security tokens and other types of tokens on the EU level. Also, potentially needs to be cleared out what types of DLT technology may be used and which requirements will apply for the specific types of the DLT networks (i.e. private, public, hybrid, etc.)

Question 98. FCD sets out rules on conflict of laws. Would you see any particular issue with applying these rules in a DLT network³²?

5000 character(s) maximum

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

Yes, we believe that such clarification would need to be in place, especially in the case of the public DLT networks. This possibly is not so much of an issue in the case of private DLT networks, where there is only a limited number of participants.

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 If you do agree that the effective functioning and/or use of a DLT solution is limited or constrained by any of the FCD provisions, please provide specific examples (e.g. provisions national legislation transposing or implementing FCD, supervisory practices, interpretation, application, ...). Please explain your reasoning.

5000 character(s) maximum

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

8. European Markets Infrastructure Regulation (EMIR)

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

Without going into the detail of specific EMIR rules, given the fact that security tokens should represent a real world asset, only in digitized form, there is no reason why such assets should not be cleared in the same way. Moreover, these assets, because of their fully digital nature, give an opportunity to do the processes, such as clearing, in a more automated way.

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on settlement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Organisational requirements for CCPs and for TRs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on segregation and portability of clearing members' and clients' assets and positions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rules on requirements for participation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Reporting requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

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.

We do not have any other strong opinions in this area.

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.

Yes. As in order legal areas, clarification, guidelines or any other rules regarding DLT and similar solutions are missing which causes legal uncertainty and hindrance for further developments.

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.

No. Cryptocurrency derivatives are already an existing phenomenon in countries outside the EU. Example: CME below. We do not see any particular issues with derivatives with underlying crypto assets.

9. The Alternative Investment Fund Directive

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

The following questions seek stakeholders' views on whether and to what extent the application of AIFMD to tokens could raise some challenges. For instance, AIFMD sets out an explicit obligation to appoint a depositary for each AIF. Fulfilling this requirement is a part of the AIFM authorisation and operation. The assets of the AIF shall be entrusted to

the depositary for safekeeping. For crypto-assets that are not 'security tokens' (those which do not qualify as financial instruments), the rules for 'other assets' apply under the AIFMD. In such a case, the depositary needs to ensure the safekeeping (which involves verification of ownership and up-to-date recordkeeping) but not the custody. An uncertainty can arguably occur whether the depositary can perform this task for security tokens and also whether the safekeeping requirements can be complied with.

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

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;	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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;	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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;	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets;	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

We do not have any other strong opinions in this area.

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.

We believe that there is no reason why the EU AIFMD legal framework could not be used for assets based on the DLT solutions. Similar rules should apply as for any other assets. The actual manner of how to fulfil certain obligations may be different (i.e. there will be different safekeeping solutions for DLT based assets than for other assets), but the obligations themselves should be the same. There is no reason to create double standards, but rather give guidance on how to comply with existing regulation in the DLT environment.

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.

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

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

For instance, under the UCITS Directive, an investment company and a management company (for each of the common funds that it manages) shall ensure that a single depositary is appointed. The assets of the UCITS shall be entrusted to the depositary for safekeeping. For crypto-assets that are not 'security tokens' (those which do not qualify as financial 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"	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
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;	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
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;	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping						

and the requirements of the depositary, as applied to security tokens;	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disclosure and reporting requirements set out in the UCITS Directive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

We do not have any other strong opinions in this area.

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.

We believe that there is no reason why the EU UCITS Directive legal framework could not be used for assets based on the DLT solutions. Similar rules should apply as for any other assets. The actual manner of how to fulfil certain obligations may be different (i.e. there will be different safekeeping solutions for DLT based assets than for other assets), but the obligations themselves should be the same. There is no reason to create double standards, but rather give guidance on how to comply with existing regulation in the DLT environment.

The only exception is the definition of a “financial instrument”, “transferable security” and similar, where we believe should be created a clear definition or guidance which comprehends digital assets, in conjunction with crypto-asset definitions created on the EU-wide level.

11. Other final comments and questions as regards tokens

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

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

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

108.1 If you do think that the EU legislation should provide for more regulatory flexibility for stakeholders to develop trading and post-trading solutions using for example permissionless blockchain and decentralised platforms, please explain the regulatory approach that you favour. Please explain your reasoning.

5000 character(s) maximum

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

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.

The main benefits are more flexibility for trading, especially for retail investors, which will also create bigger financial inclusion, globalization of the markets, and lower costs. There is a strong push among certain players towards decentralized finance, i.e. DeFi, already. Basic definition can be found for example here: <https://www.binance.vision/glossary/defi>

Some of the risks may include technological risks (i.e. platform hacking, or risks connected to the decentralized DLT technology, e.g. 51 per cent attacks or weak coding, etc.) and potentially regulatory compliance risks, especially during the time, when regulation is behind the current developments and the market players do not have in this regard clear guidance and legal certainty.

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

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

- 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.

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.

We feel that the biggest hindrance for the further development in this area are missing common EU-wide definitions of crypto assets, which should be a start.

As an example of overly defensive/conservative legislation we can give the AML law in the Czech Republic, which stated that the “obliged entity” under such law is any company which does any business in relation to crypto-assets. These overly conservative catch-all clauses which tend to regulate everything are the very reason why some innovative companies cannot flourish as they are burdened by extensive legal requirements.

C. Assessment of legislation for ‘e-money’ tokens

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

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

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

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

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

- 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.

We do not have any strong opinions in this area.

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.

We do not have any strong opinions in this area.

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 potential use of DLT technology for e-money should not create a double standard when applying the EMD2 or PSD2 rules. This would only further complicate this area of regulation.

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

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Safeguarding requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Issuance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Redeemability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Use of agents	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Out of court complaint and redress procedures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

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.

We do not see any other requirement under EMD2 that would be appropriate for “global stablecoins”.

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.

Although we do agree that in the case when stablecoins would fall under the definition of e-money, it should comply with all the necessary requirements and not create a double standards, we also believe that guidance on how to assess whether a stablecoin is also “e-money” is needed for legal certainty of the market players.

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.

When a clear distinction between “e-money tokens” and “stablecoins” is made, we are of the opinion that it is not a problem to have different rules for each of the categories. Stablecoins, with the use of novel technologies, may come up with even better payment safeguards than set up by the PSD2 requirements. So in order not to stifle the innovation in this sector, we would not recommend to put it under the rules of PSD2 completely. Although the safety standards for payments with stablecoins should not be lower than with the other (more traditional) payments means, PSD2 was drafted with the focus on a rather different technological background, so it may not be always applicable especially to DLT environments.

Additional information

Should you wish to provide additional information (e.g. a position paper, report) or raise specific points not covered by the questionnaire, you can upload your additional document(s) here:

The maximum file size is 1 MB.

You can upload several files.

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

Useful links

[More on the Transparency register \(http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en\)](http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en)

[More on this consultation \(https://ec.europa.eu/info/publications/finance-consultations-2019-crypto-assets_en\)](https://ec.europa.eu/info/publications/finance-consultations-2019-crypto-assets_en)

[Specific privacy statement \(https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement_en\)](https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement_en)

[Consultation document \(https://ec.europa.eu/info/files/2019-crypto-assets-consultation-document_en\)](https://ec.europa.eu/info/files/2019-crypto-assets-consultation-document_en)

Contact

fisma-crypto-assets@ec.europa.eu