

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

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

⁸ G7 Working group on "stablecoins", [Report on 'Investigating the impact of global stablecoins'](#), October 2019

⁹ [Speech by Vice-President Dombrovskis at the Bucharest Eurofi High-level Seminar](#), 4 April 2019

¹⁰ [Mission letter of President-elect Von der Leyen to Vice-President Dombrovskis](#), 10 September 2019

¹¹ Joint Statement of the European Commission and Council on "stablecoins", 5 December 2019

¹² Those crypto-assets are currently unregulated at EU level, except those which qualify as 'virtual currencies' under the AML/CFT framework (see section I.C. of this document).

Please note: In order to ensure a fair and transparent consultation process **only responses received through our online questionnaire will be taken into account** and included in the report summarising the responses. Should you have a problem completing this questionnaire or if you require particular assistance, please contact fisma-crypto-assets@ec.europa.eu.

More information:

- [on this consultation](#)
- [on the consultation document](#)
- [on the protection of personal data regime for this consultation](#)

About you

* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- Gaelic
- German
- Greek
- Hungarian
- Italian
- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese

- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

- | | | |
|---|---|--|
| <input type="radio"/> Academic/research institution | <input type="radio"/> EU citizen | <input type="radio"/> Public authority |
| <input checked="" type="radio"/> Business association | <input type="radio"/> Environmental organisation | <input type="radio"/> Trade union |
| <input type="radio"/> Company/business organisation | <input type="radio"/> Non-EU citizen | <input type="radio"/> Other |
| <input type="radio"/> Consumer organisation | <input type="radio"/> Non-governmental organisation (NGO) | |

* First name

* Surname

* Email (this won't be published)

* Country of origin

Please add your country of origin, or that of your organisation.

- | | | | |
|--------------------------------------|--|-------------------------------------|--|
| <input type="radio"/> Afghanistan | <input type="radio"/> Djibouti | <input type="radio"/> Libya | <input type="radio"/> Saint Martin |
| <input type="radio"/> Åland Islands | <input type="radio"/> Dominica | <input type="radio"/> Liechtenstein | <input type="radio"/> Saint Pierre and Miquelon |
| <input type="radio"/> Albania | <input type="radio"/> Dominican Republic | <input type="radio"/> Lithuania | <input type="radio"/> Saint Vincent and the Grenadines |
| <input type="radio"/> Algeria | <input type="radio"/> Ecuador | <input type="radio"/> Luxembourg | <input type="radio"/> Samoa |
| <input type="radio"/> American Samoa | <input type="radio"/> Egypt | <input type="radio"/> Macau | <input type="radio"/> San Marino |
| <input type="radio"/> Andorra | <input type="radio"/> El Salvador | <input type="radio"/> Madagascar | <input type="radio"/> São Tomé and Príncipe |
| <input type="radio"/> Angola | <input type="radio"/> Equatorial Guinea | <input type="radio"/> Malawi | <input type="radio"/> Saudi Arabia |
| <input type="radio"/> Anguilla | <input type="radio"/> Eritrea | <input type="radio"/> Malaysia | <input type="radio"/> Senegal |
| <input type="radio"/> Antarctica | <input type="radio"/> Estonia | <input type="radio"/> Maldives | <input type="radio"/> Serbia |

- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar /Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago

- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

* Organisation name

255 character(s) maximum

ESBG (European Savings and Retail Banking Group)

* Organisation size

- Micro (1 to 9 employees)
- Small (10 to 49 employees)
- Medium (50 to 249 employees)
- Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the [transparency register](#). It's a voluntary database for organisations seeking to influence EU decision-making.

8765978796-80

* Field of activity or sector (if applicable):

at least 1 choice(s)

- Asset management
- Banking
- Crypto-asset exchange
- Crypto-asset trading platforms
- Crypto-asset users
- Electronic money issuer
- FinTech
- Investment firm
- Issuer of crypto-assets
- Market infrastructure (e.g. CCPs, CSDs, Stock exchanges)
- Other crypto-asset service providers
- Payment service provider
- Technology expert (e.g. blockchain developers)
- Wallet provider
- Other
- Not applicable

* At the benchmark level, I am giving my contribution as a:

- Benchmark administrator
- Benchmark contributor
- Benchmark user
- Other

* Please specify under what benchmark-related status you are giving your contribution:

We are an European Association of Saving and Retail banks

* Publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

Anonymous

Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.

Public

Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

I agree with the [personal data protection provisions](#)

I. Questions for the general public

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

Question 1. Have you ever held crypto-assets?

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

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

- Yes
- No
- 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.

Regulations should be the same for identical/similar functional or business purposes.

Most digital assets per se have the same functioning and features of the physical version of the same assets, with the only difference being in the digital channel for its distribution. Crypto-assets require a specific assessment, initiative and regulatory response, due to the fact that they apparently have additional distinguishing features.

As a technology-neutral approach should be the objective, it would be too early to constrain on cryptography as a technology (which is imminent when limiting to crypto-assets in the given approach) and to start off with such an approach. This would not ensure that regulations are really technology-neutral and that a functional /business point of view is taken at the end, supporting a level playing field through legal clarity. However, as it will be discussed throughout our response to this questionnaire, not even crypto-assets are so distinct from the physical version of the assets.

Crypto-assets and digital assets comprise different risks and require a separated analysis and treatment. A general scope including all digital assets would be therefore inefficient from a regulatory perspective.

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.

Prior to determining any classification of crypto-assets, a legal definition is needed.

A general framework for both the definition and the classification of crypto-assets should be set-up through regulatory measures; to ensure that a scope expansion of crypto-assets is done in a harmonized manner across current legislation. Regulatory measures provide a level playing field for the market participants involved. Furthermore, market players will need a more detailed non-legislative guidance, probably from the ESAs, including concrete examples and use-cases indicating how the different categories of crypto-assets can be classified.

Any regulatory policy should take into account the various purposes/functions of crypto-assets. In order to differentiate between the various purposes/functions, and to provide for a clear legal framework for crypto-assets, a classification is needed and should be implemented into the relevant legal framework to be applied to crypto-assets.

In addition, regulatory classification as digital/crypto-assets and their business models should be global, not local, and regulatory arbitrage should be prevented.

Such a provided classification at EU level should underpin a legal regime for services on crypto-assets. In other words, we need to define different types of crypto-assets in order to allow the application of differentiated rules, appropriate to each type of crypto-assets, and dependant on their specific nature.

In addition, we believe that such classification should be flexible enough to accommodate for technological progress and that a transitional regime could enable the emergence of a detailed classification. At first, EU supervisors and NCAs need to take initiatives and provide guidance, then EU legislators should enlarge the scope through a general /high level classification and finally provide with regulation for those areas of the crypto-assets that do not fall under EU legislation.

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.

Similar to Swiss FINMA or Singapore MAS and embedding in already existing respective regulations. EU regulator should restrain from creating new ones. Especially, the classification shall ensure that, where necessary, existing regulation can be easily applied instead of unnecessary introduction of new concepts. A

taxonomy/classification will also ensure proper differentiation between (digital/crypto) assets that are de-facto already regulated (as e.g. they can be classified as financial instruments due to their economic function) and those which are not regulated yet.

We believe that such classification should be harmonised at European level so that a passporting regime can be established and at the same time be flexible enough to accommodate technological progress.

For example, in France, crypto-assets are split into two categories: crypto-assets which fall under existing EU regulation and those which do not. A new regulatory framework has recently been introduced (through PACTE law) for the latter, including assets which do not qualify as “financial securities” as per MiFID2 (Annex 1, section C).

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

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

Question 8.1 If you do agree that any EU classification of crypto-assets should make a distinction between ‘payment tokens’, ‘investment tokens’, ‘utility tokens’ and ‘hybrid tokens’, please indicate if any further sub-classification would be necessary:

5000 character(s) maximum

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

Regulatory policy should take into account the various purposes/functions of crypto-assets. Depending on the individual function/purpose of a crypto-asset, different aspects have to be considered. While e.g. payment tokens may raise questions of depositor and consumer protection as well as issues related to payment services, investment tokens may raise questions of investor protection.

We believe that there should be three categories:

1. Security tokens which correspond to financial instruments as defined and regulated by MiFID (keeping in mind the specific requirements of CSDR regarding listed transferrable securities); and
2. Other crypto-assets, which currently fall outside of the existing EU regulation namely:
 - a. utility tokens
 - b. crypto currencies

One risk is that many assets could fall within the category of utility tokens. If regulatory rules depend on the classification, this easily can become a problem. In our current understanding the hybrid categories are very broad and creating a situation where tokens that are difficult to classify into a regulated category would require a case-by-case approach – requiring input from supervisors.

It is rather important to define the overall approach that should be followed: Any classification scheme should be embedded in current existing schemes to keep current differences in regulations between e.g. fungible and non-fungible financial instruments.

To summarize, the classification proposed in the question makes in general sense, but it is not clear whether

or not it is the best or “primary” classification. We therefore strongly recommend to scan existing regulation and law for already immanent classifications in order to establish at which level the digitalization aspects can and have to be addressed first.

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.

Our main concerns come from "hybrid tokens", because it is not clear why they would constitute a separate category of crypto-assets. They need specific clarifications regarding how the different rights emanating from those assets play a role in the allocation of rights and obligations. However, considering them a separate category raises doubts. Therefore, it is important that the industry receives clear guidance from supervisors to ensure harmonization and high levels of consumer protection.

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.

Currently, ESBG has not identified any crypto-asset marketed or considered as ‘deposit’. However, the potential deposit of encrypted assets could be possible in the future. In such a case these assets should be subject to the banking regulatory framework in particular, if they have the characteristic or the core feature of legal tender.

In case the Commission or any respondent observes "deposit tokens" marketed, and subsequent regulatory measures are taken, we would ask the Commission to provide examples and use cases in a transparent manner. We find it difficult to understand how the use of a token can make any difference to how banking "deposits" work under the DGSD.

In any case, ESBG considers that only payment tokens should be considered if they fulfil the requirements in the DGSD and other legislations such as AML.

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)

	1 (not important at all)	2	3	4	5 (very important)	Don't know / no opinion / not relevant
Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Issuance of utility tokens as an alternative funding source for start-ups	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cheap, fast and swift payment instrument	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enhanced financial inclusion	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Crypto-assets as a new investment opportunity for investors	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Improved transparency and traceability of transactions	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Enhanced innovation and competition	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Improved liquidity and tradability of tokenised 'assets'	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enhanced operational resilience (including cyber resilience)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security and management of personal data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input 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 checked="" type="radio"/>	<input 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.

Regulatory requirements (AML/CFT, KYC, MiFID2/MAD2, PSD2, etc.) and respective necessary technical amendments will outweigh the currently experienced 'easy' go to market and consumer experience. But new technology can also offer solutions to for instance money laundering and simultaneously enhance financial inclusion and reduced costs of fundraising.

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.

The potential benefits related to crypto-assets are significant, in particular in terms of efficiency. Liquidity could also be potentially increased by giving an access to some assets to smaller investors. One other benefit we see is the ability for an Equity/Bond issuer or an investment manager to have to have access to the investor registry that is updated in real time. Finally, ICOs are an interesting alternative for companies to raise funds, compared to current funding tools.

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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Market integrity (e.g. price, volume manipulation, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Investor/consumer protection	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Anti-money laundering and CFT issues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Energy consumption entailed in crypto-asset activities	<input type="radio"/>	<input type="radio"/>	<input checked="" 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.

The international dimensions of crypto assets place great responsibility on global coordination and harmonization between policy makers and supervisors to achieve the full potential of these new

technologies. DLT technology also creates GDPR challenges as information cannot be deleted. These are challenges that either regulation or technology can contribute to solve.

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.

In the longer term, if crypto assets can be used for retail payments, this can have implications on the current monetary policy and financial stability – especially if the funds are no longer deposited with a credit institution but instead stored in other places. This would increase funding costs and increase the risk of bank runs.

It is key to preserve and extend to crypto-assets market recent advances and improvements achieved in market integrity, investor and data protection, and anti-money laundering

In general, all risked activities depend on the technical implementation, like existing financial systems and products. You find equivalents to existing risks from the 'centralized world' in the 'decentralized ecosystems'. The technologies and usage of technologies is in an early stage, so all risks of new technologies are relevant.

"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.

Stablecoins also offer opportunities to make the payment system more efficient and contribute to the development of faster, cheaper and more inclusive global payments. They are also expected to provide stability to their market price. However, the mechanism through which that stability is to be provided has still not been proved in any jurisdiction by any provider. Further, as all stablecoins have the potential of becoming global it is difficult to make a distinction between global and non-global.

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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Market integrity (e.g. price, volume manipulation...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Investor/consumer protection	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Anti-money laundering and CFT issues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Energy consumption	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Financial stability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Monetary sovereignty/monetary policy transmission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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.

The risks of not applying the principle of same services, same risks, and same rules are great. For instance, if stablecoins are used for payment transactions they should fall under the same scrutiny as all other

payment products especially concerning risks related to AML, KYC and other legal requirements such as PSD2. Regulators and policy makers also need to take the systemic risks into consideration to ensure that the build-up of systemic risks are mitigated.

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.

Given the digital nature of all stablecoins it is difficult to make a distinction between the two. The so called global stablecoins are designated as such because of their ability to reach global scale in a quick manner, thanks to the existing massive customer base of their providers. ESGG agrees that the potential global dimension of stablecoins can have an exponential effect on the risks to financial stability, market integration, the transmission of monetary policy measures, and issues related to unfair competition.

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.

Good regulation is necessary, but we should just scope the assets into current regulation as a quick fix. Same service, risks and rules. A bespoke regime is only required if crypto assets fall outside of the current regulatory scope. We believe that this should not be the case. Otherwise we have a situation as currently, i.e. no regulation, unclear and chaotic markets/environments and therefore very limited acceptance by very few market participants.

A bespoke European framework provides legal certainty and prevents a race to the bottom by regulatory arbitrage and should guarantee a level-playing field in financial services markets.

A bespoke regime for crypto-assets would enable the development of a crypto-asset ecosystem in the EU. This regime should be attractive for industry players, provide legal certainty, and ensure an adequate level of protection for consumers and investors. It should also be flexible enough to accommodate technical

progress.

The European regulation should introduce a passporting regime allowing activities relating to crypto assets to be performed from one Member State throughout the whole EU.

Furthermore, we are of the opinion that a transitional and harmonised regime at European level allowing experimentation in this field, while waiting for the finalisation of such bespoke regime, would be very beneficial.

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.

As an example, we take note of the measures included in the French PACTE law which could be an effective approach to crypto-assets regulation. Indeed, the French regimes for ICOs and Digital Asset Service Providers (DASPs) allows both enough flexibility for entrepreneurs to develop their ideas – in particular through the optional nature of the visa - and an appropriate level of protection for investors – thanks to the supervision of the AMF: the visa reflects both recognition of reliability and protection, both for investors and issuers. And this regime is simple - the AMF is the single point of contact for ICO issuers and DASPs and the sole competent body for granting the visa.

The AMF publishes a list of registered service providers and of ICOs which received its visa on its website, making this regime attractive for industry players as well as investors and consumers.

As an example, we could also consider the case of Crypto custody license according to Gesetz für das Kreditwesen (KWG) in Germany:

We welcome the law implementing the Fourth EU Money Laundering Directive, as this defines for the first time crypto assets and introduces the regulatory classification of crypto assets as a new financial instrument in KWG in Germany. The Act implementing the Amending Directive to the Fourth EU Money Laundering Directive (BGBl. I as of 19 December 2019, p. 2602) came into force on 1 January 2020. This means that the new transitional provision of § 64y KWG applies to all companies that are subject to the definition of crypto-custody business in the new § 1 (1a) sentence 2 no. 6 KWG when the law comes into force. Under the conditions of section 64y KWG, the licence required since the law came into force is provisionally deemed to have been granted to these companies. As a result, irrespective of the date of submission of the notification of intent, these companies are obligated under money laundering law as of 1 January 2020 within the meaning of § 2 (1) of the Money Laundering Act (GwG).

Another example: It is possible to issue and post-process, on DLT, a Schuldscheindarlehen as non-transferable asset. Then the same regulatory terms should be applied to this case just as with any other “conventional” Schuldschein (which is e.g. not a financial instrument) or any other form of digitization of a Schuldschein (e.g. based upon non-DLT technology).

In the absence of an ad-hoc regulation in Spain, the National Securities Market Commission (CNMV) has

proportionated a framework to market participants and addressed consultations by private agents. For example, CNMV assimilates the issuance of crypto-currencies and tokens to the issuance of financial instruments. Therefore, it requires the compliance with the obligations established in the Securities Market Law, for example, the presentation of a prospectus, the maintenance of an accounting record and the assumption of various responsibilities

Final Settlement Directive: It should be clarified that Directive 98/26/EC on settlement finality (Finality Directive) is also applicable to DLT-based booking systems of crypto-assets in order to enable the legal effectiveness and insolvency-proof nature of transactions processed through such booking systems transfers and corresponding orders. Furthermore, we advocate the prompt dematerialisation of securities and, as a result, the accompanying enabling of security tokens under German law.

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.

Any sort of regulatory measures on crypto-assets would require an assimilation to the current consumer protection legislation. As a first step, we advocate to adapt the current legislation to accommodate crypto-assets.

Existing regulations should amend their definitions to cover also respective digital/crypto-asset types, e.g. payment tokens with PSD2, AML/CTF, security tokens with MiFID2/MAD2/etc.; all respective risk regulations are applicable as well. See, however, remarks in the answer to Question 8.

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.

In terms of the prudential treatment of crypto-assets in the banking sector, it needs to be taken into account that, based on the characteristics of each asset, different risks are involved in a crypto-asset. Greater clarity regarding the prudential treatment of crypto-assets could help financial institutions to use the potential of this market. For example, some of the risk that exposures to crypto-assets may face are the following: counterparty credit risk, market risk, operational risk, credit risk, liquidity risk and exchange rate risk.

However, we consider that the risks, to which banks can be exposed, may differ depending on whether the crypto-asset is in custody on behalf of a customer (off-balance sheet) or owned by the bank (on-balance sheet).

Based on the risks involved, regulatory and supervisory authorities should take a decision on the necessary capital requirements that should be associated with them. It is of paramount importance that not all exposures to crypto-assets are treated in an equal manner. Different assets entail different risks, and thus they should be linked to different capital requirements. The Basel Committee on Banking Supervision is already taking steps on this issue. It is therefore important that any efforts are coordinated at international level to ensure a level playing field across different countries and jurisdictions.

17.1 Please explain your reasoning for your answer to question 17:

5000 character(s) maximum

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

Question 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.

Yes. A harmonization and clarity of the regulatory approach on EU level will only work out if the underlying definitions and approaches to digital/crypto assets and financial instruments are also harmonized.

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.

Across Europe we can find services providers relating to exchange, trading platforms and wallet providers of crypto-assets.

In addition, and as an example, the PACTE law has created the DASP status which allows ac-tors to provide the following services on digital assets (crypto currency and utility tokens).

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.

The answer is meant in a very general sense. This does not mean that existing cross-border provisions should be altered or not apply specifically for digital/crypto-assets. It should be taken into account that certain legislation requires physical presence, such as for instance MiFID II which requires presence to service retail clients in the EU.

Yes, we believe that the issuer or sponsor of crypto-assets marketed to EU investors/consumers should be established or have a physical presence in the EU. Indeed, this will ensure an appropriate level of protection of EU investors/consumers, as EU authorities only have jurisdiction on entities established in the EU territory. Moreover, this will contribute to attract crypto-assets activities in the EU.

More specifically, issuers or sponsors of crypto assets marketed to EU investors/consumers should comply with substance requirements, in line with ESMA's general opinion published in May 2017[1] and proportionate to their activities.

In order to build a single market and ensure the development of crypto-asset activities, the EU framework for markets in crypto-assets should include a passporting regime allowing issuers and sponsors to market their crypto-assets throughout the whole EU, i.e. an issuer or sponsor established in one Member State should be authorised to market its activities in the 27 EU Member States.

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.

Currently there is a plethora of possibilities to issue digital/crypto-assets. The associated risks and questions are not always answered within the current prospectus approach.

Existing regulations shall be applied and the content shall be as comprehensive as possible, covering not only traditional asset information but also crypto-asset specific information (such as outlined in the question).

The issuer / sponsor should be responsible for the disclosure.

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 type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The E-Commerce Directive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The EU Distance Marketing of Consumer Financial Services Directive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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.

Existing regulations which shall apply to token types as outlined above.

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.

Legislative modifications

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 type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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.

Similar to traditional assets.

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.

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.

Global aspect is covered only if crypto-asset is :

1. accepted in all major economic regions for payment/investment/utility
2. convertible from/to national FIAT similar to other FIAT in all major economic regions

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"/>
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"/>
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 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"/>
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.

Tools to better combat AML challenges with current crypto-assets.

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.

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.

25.2 b) Please Please illustrate your responses to question 25.2:

5000 character(s) maximum

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

“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.

It is too early to answer this question as without an indication how the regulatory treatment is intended this cannot be answered. However, in general, consumer / investor protection rules should not be applied to wholesale stablecoins. The rest of the risks are present and measures on data protection, cybersecurity, competition, etc. should be taken.

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 type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 checked="" type="radio"/>	<input 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 type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Lacks of resources to effectively conduct its activities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 checked="" type="radio"/>	<input 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 type="radio"/>	<input checked="" 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.

Lack of regulatory clarity and transparency can lead to mispricing, building up of risks and creating opportunities for market manipulation.

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.

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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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.

No matter the characteristic of the crypto-asset, i.e. centralized or distributed, there needs to be a framework in place to ensure that public institutions can identify the build-up of risks and apply mitigation 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.

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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 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 exchange	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Inadequate own funds to repay the consumers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Losses of users' crypto-assets through theft or hacking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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.

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.

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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Exchanges should be subject to advertising rules to avoid misleading marketing/promotions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input checked="" 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.

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.

In relation to crypto-assets custodial services it is important to take into account the legal status of private keys and their custody.

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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Absence or inadequate segregation of assets held on the behalf of clients	<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 (trading, exchange)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 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 custodial wallet provider	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Inadequate own funds to repay the consumers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The custodial wallet provider behaves negligently or fraudulently	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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.

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.

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)

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

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	no opinion / not relevant
Custodial wallet providers should have a physical presence in the EU	<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 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 type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions	<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 certain minimum conditions for their contractual relationship with the consumers/investors	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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.

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.

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.

Crypto-assets which qualify as financial instruments under MiFID II, should be under custody according to UCITS rules and through a provider that complies with MiFID II/UCITS rules, if required current regulation for depositaries and custodians should be further adapted (UCITS Directive).

We consider that the European Union should avoid arbitrage and ensure a level playing field, but crypto-assets should be always regulated. In addition, Wallet providers should meet the same requirements as any other type of custodian of money or financial instruments.

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.

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

We do not see any reason to potentially state that any business model or service related to digital wallets should not be in the regulated space. All of them should be.

Nevertheless, the following services should be forbidden due to either inherent unmanageable high-risk nature and/or money-laundering and terror-financing enablement:

- derivatives on crypto-assets
- mixing services
- anonymous cryptocurrencies
- anonymous wallets
- anonymous payment services

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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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.

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.

Most of them are services that could fall under MiFID II. So, as those in MiFID II were included in order to protect consumers from several risks, the same risks need to be mitigated with the services indicate in Q35.

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.

Yes, in a technology neutral environment the focus should be on how the assets are used. If it is used to perform a payment, then it should be covered by PSD2 and other legislation such as AML. This allowing for a level-playing field and giving supervisors the correct tools to act and mitigate risks.

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 checked="" type="radio"/>	<input 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 checked="" type="radio"/>	<input 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.

See full list of offences in the Market Abuse Directive.

Crypto-assets which serve as an investment token are another technological representation of securities. Furthermore, any regime regulation DLT-based assets trading needs to safeguard investors against any manipulation of the underlying assets.

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.

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.

There should be no difference as to how securities are currently regulated. Technologies such as DLT need to be applied to improve market efficiency, transparency and investor protection. Therefore, they should be included in current legislation and supervisory requirements to ensure that the benefits of new technology benefits society as a whole.

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

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

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

If you see the need for supervisors to be able to formally identify the parties to transactions in crypto-assets, please explain explain how you would see this best achieved in practice:

5000 character(s) maximum

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

KYC-AML checks and measures, such as those related to enhanced due diligence. These new types of assets also need to have effective market supervision, an authorization process and reporting requirements to the NCAs to ensure proper supervision.

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.

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.

Similar to existing regulations and regimes.

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.

Yes, this is a very important tool in the fight against money-laundering and terrorist-financing. Legislation also needs to become future proof to ensure that new applications of technology in this area fall in the scope of, for instance, AML.

The term "virtual currency" is not appropriate, we would rather keep the taxonomy we adopted in question 8 above with the definition of crypto-assets.

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

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

5000 character(s) maximum

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

Yes, please see reply to question 34 and all the services included in question 35

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.

As explained in the BCBS Discussion Paper on the prudential treatment of exposure to crypto-assets, there are more channels for that exposure than the ones identified in the current EU AML/CFT framework, and even more than those identified by the FATF. If all those services entail an exposure to crypto-assets and their risks, then they should be included in the AML / CFT framework.

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.

Yes, but we still believe that there is a need for a bespoke framework on crypto-assets, but as priority rather than as an expansion of current legislation, to ensure that these assets are included. Society needs to use the technological advances to strengthen the economic system to avoid future challenges. This could make actions against AML cheaper and more efficient.

Guidelines/standard procedures including details on their practical implementation should be issued at European level. These procedures shall be adapted to the crypto-assets eco-system. Regulators at a national level should then be able to provide crypto-asset service providers with adapted guidelines that would match their own requirements.

In the regulated financial eco-system, procedures currently in place to ensure respect of the AML-FT requirements are not necessarily transferrable to the world of crypto-assets. For example: Fircosoft is not able to track crypto-asset transactions.

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.

Correctly identifying the parties involved in a transaction, which requires rules on KYC checks on the providers of the technology supporting P2P transactions. It is of great importance that all types of platforms /actors (not only banks) are in scope for both legislation and supervision. Also see response to question 34.

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.

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.

To lower risk providers of services and their leadership related to crypto-assets should be covered by the same regulations/requirements as financial institutions.

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 type="radio"/>	<input type="radio"/>	<input checked="" 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.

Crypto-assets require, as under MiFID II rules, an evaluation of the user's capacity of repayment and their understanding of the products and services they are about to buy or agree to. Therefore, suitability checks and tests as those established by MiFID II should be regarded.

Information requirement should be calibrated to relevant investment amount. The issuer should probably issue a warning on the risks associated to the tokens issued.

Suitability checks by the crypto-asset service providers (including exchanges, wallet providers...): It makes sense to implement a suitability check in case of advisory circumstances.

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.

Such requirements should apply to all types of crypto-assets offered to retail end-consumers.

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.

Consumer/investor protection standards should not be different, but of different magnitude or be applied with a risk-based approach. It should be the end consumer/investor who is in focus not the asset. Standards of consumer/investor protection should be adapted in terms of risk.

Regulatory policy should take into account the various purposes/functions of crypto-assets. The specific risks for consumers/investors depend on the individual purpose/functions of the re-spective crypto-asset.

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

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

- 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.

MiFID II, classifications of different clients should be used i.e.: retail, professional, eligible counterparties.

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.

More of a tax question

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	2	3	4	5 (very relevant factor)	Don't know / no opinion /
--	---	---	---	---	-----------------------------	---------------------------

	(factor not relevant at all)					not relevant
Those crypto-assets should be banned	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input 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.

To limit the challenges of this, frameworks need to be created on an international level. We believe that there should be no prohibition on crypto-assets issued in third countries, rather, restrictions inspired from the world of financial assets, such as the qualification of investors, should be put in place.

We believe that an equivalence regime is suitable, and this regime should provide specific warnings aimed at consumers when equivalence is not met.

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.

Same service, same risks, same rules.

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.

All crypto-asset service providers need to be subject to supervisory coordination or supervision by the ESAs in cooperation with the ESCB where relevant.

- custody of digital assets, meaning in practice the custody of cryptographic keys on behalf of a client;
- the service of buying or selling digital assets for legal tender;
- the service of trading digital assets for other digital assets;
- the reception and transmission of orders for digital assets, meaning the act of receiving and transmitting buy or sell orders for digital assets on behalf of a client;
- the management of digital asset portfolios, meaning the act of managing, on a discretionary, client-by-client basis, portfolios that include one or more digital assets under a mandate given by a client;
- advice to investors in digital assets. This means giving personalized recommendations to a third party, either at their request or on the initiative of the service provider providing the advice, concerning one or more digital assets;
- digital asset underwriting, meaning the act of purchasing digital assets directly from a digital asset issuer, with a view to subsequently selling them;
- the guaranteed investment of digital assets, which consists in searching for buyers on behalf of a digital asset issuer and guaranteeing them a minimum amount of purchases by undertaking to buy any digital assets that are not placed;
- the unsecured investment of digital assets, meaning the act of searching for buyers on behalf of a digital asset issuer without guaranteeing them an amount of purchases; and
- the operation of a trading platform for digital assets. This concerns the management of one or more digital asset trading platforms, within which multiple buying and selling interests expressed by third parties for digital assets in exchange for other digital assets or a currency that is legal tender can interact in such a way as to result in the conclusion of contracts.

By its nature, business related to crypto-assets has a global scale. Addressing the risks they entail (market integrity, AML or tax evasion) requires international cooperation from regulators and supervisors. Since access to crypto exchanges is as easy as a “click”, consumer and investor protection for crypto exchanges would benefit from a global approach. We therefore consider that, in Europe, the European Supervisory Authorities should play a key role in the area of supervision, together the ECB and NCBs.

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.

Cybersecurity and ICT risks, data protection management, transparent and fair consumer protection practices, and proper AML/CFT and KYC checks.

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.

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.

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.

There is no increased risk if the same regulatory legal framework is there.

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.

Yes

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.

Start full regulation now by fully integrating crypto-assets into existing corresponding regulations, otherwise uncertainties and high risks remain.

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.

It is necessary to have a common regulatory and supervisory approach for security tokens in the EU. This would avoid diverging conclusions on what should be considered a security token across the different jurisdictions and national regulatory frameworks.

More precisely, we urge the European regulator to implement some transition regime which would allow some exemptions from the existing European regulations which are not appropriate to crypto-assets.

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 type="radio"/>	<input checked="" 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 type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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.

Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token:

We are in favour of a common regulatory framework in the EU. Therefore it would be most effective to implement a specific regulation.

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 checked="" type="radio"/>	<input 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.

The idea of classification should be revisited. It is unclear whether the idea of classification in security, utility etc. tokens is the optimal one. Care must be applied to keep current differences in regulation between e.g. fungible and non-fungible financial instruments and to properly extend them to digital/crypto-assets.

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.

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.

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.

A guidance is just sufficient as a preliminary step. The second step should be a regulatory framework.

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.

The current scope is overall appropriate, but some adjustments should be made, as changes to adapt the legislation to the specificities of these new instruments.

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.

A Directive is certainly not the best tool to create a common European basis for such a new progressive technology.

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

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

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

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

Please explain your reasoning.

5000 character(s) maximum

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

Yes

In case of permissionless distributed ledgers, the question of accountability must be specifically addressed.

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, they are appropriate, but the current rules need some adaptations to the specificities of security tokens. The general principles in the regulatory framework should apply to security tokens, in any case, as the nature of the transactions and the position of retail investors is essentially the same.

As the wording of security token is used: If classification is set up based on concepts of security and utility tokens (as outlined in question 8) and rules are only applied to security tokens, we see the danger that a level-playing field of regulation is actually not realized as many tokens might be classified in the grey area of utility tokens.

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.

No, should be similar to traditional securities. But the constraint to security tokens is problematic (see answer to question 8).

It is important that potential investors can get a detailed overview before purchasing a security token. Investors must therefore be provided with information material that shows not only the opportunities but also the specific risks.

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.

No, but the constraint to security tokens is problematic (see answer to the first questions)

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

Less costs, more flexible “securitization” via “tokenization”. Integration in other offerings by re-using DLT infrastructure and tokens into SMEs products/services.

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.

No. All measures and requirements that are in place for the traditional market, should be in foreseen for security tokens as well. Otherwise a regulatory arbitrage will occur.

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.

Only to the Smart Contracts aspects, which need to be properly reflected.

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.

The same (if similarly regulated) as with trading venues.

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.

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

5000 character(s) maximum

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

No

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.

No. In order to maintain market integrity and to prevent market abuse and insider trading, the same rules should apply for security tokens.

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.

If the security token is traded on venues regulated under MiFID rules, then those rules should be applied in terms of insider information and dealing.

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. The definition already covers market manipulation related with security tokens.

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.

No (if similarly regulated)

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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Restrictions on uncovered short selling	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input 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 checked="" type="radio"/>	<input 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.

Not yet.

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.

If security tokens are qualified as financial instruments, SSR would also capture them. Although it might be more difficult to detect short selling that is unlawful due to the decentralised system of acquirement and disposition of security tokens, the implementation of comparable rules seems feasible.

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.

Not yet.

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.

In particular, we do not consider the following exceptions to be relevant: Art. 1 (3) para.4 e), f), g), h), j); para 5 b)), d), g), i). However, future developments may require additional exemptions.

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.

Yes, we are in favour of the building block approach.

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, but if security tokens are considered financial instruments, they should be required to obtain an ISIN.

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.

No

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.

We do not consider that an ad hoc alleviated prospectus type or regime should be created. There is no reason to treat security tokens as privileged compared to common securities

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.

A regulated regime for crypto-assets is the very foundation for any kind of sustainable (crypto-) asset regime. Otherwise we have a situation as currently, i.e. no regulation, unclear and chaotic markets/environments and therefore very limited acceptance by very few market participants.

We are of the opinion that the ESMA guidelines should be adapted with regard to the particular DLT risks.

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 checked="" type="radio"/>	<input type="radio"/>	<input 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 checked="" type="radio"/>	<input type="radio"/>	<input 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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Definition of 'book-entry form' and 'dematerialised form'	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input 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 checked="" type="radio"/>	<input 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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
What entity could qualify as a settlement internaliser	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input 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.

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.

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.

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.

Tokens should fall under an European Regulation, not a Directive or divergent national laws.

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

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.

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.

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

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.

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.

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

5000 character(s) maximum

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

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

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

96.1 Please explain your reasoning for your answer to question 96:

5000 character(s) maximum

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

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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If records on a DLT qualify as relevant account	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input 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.

97.2 Please explain your reasoning for your answer to question 97:

5000 character(s) maximum

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

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

5000 character(s) maximum

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

No

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.

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

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

100.1 Please explain your reasoning for your answer to question 100:

5000 character(s) maximum

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

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.

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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Rules on settlement	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

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.

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

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

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)

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

	1 (not suited)	2	3	4	5 (very suited)	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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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.

105.2 Please explain your reasoning for your answer to question 105:

5000 character(s) maximum

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

The depository function will be necessary for safeguarding private keys. Therefore, the appointment of specialised depositories able to take custody of security tokens is necessary to provide the required security to the market

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 depository is appointed. The assets of the UCITS shall be entrusted to the depository 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 depository 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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 type="radio"/>	<input checked="" 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.

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.

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

108.2 Please explain your reasoning for your answer to question 110:

5000 character(s) maximum

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

Regulations should not be more flexible depending on the technology used for delivering a service. Existing regulations should be similarly applicable. The same services should be subject to the same regulation, regardless of the technology used for providing it.

In general, we have a well-balanced system with rules for investment firms, trading venues, CCPs and CSDs. All these players need a permission to operate and are subject to supervision by the competent authority. Although it might be possible in theory to operate without permission, the system to ensure financial stability would be put at risk if there are players without permission in the market. Besides that, this would harm a fair competition in which the best quality should be successful and not the least regulated.

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.

No major benefits, only all already known risks at a higher level due to it being “permissionless”.

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.

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.

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.

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.

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.

Supervisory guidance is required, in order to clarify how e-money tokens such as stablecoins will be supervised by EU authorities.

In addition, the definition section for payment instruments should be amended accordingly.

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.

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.

The requirements under EMD2 do not address the systemic risks of global stablecoins.

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.

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