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, 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 value. 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 2009. There are many ways to classify the different types of crypto
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 pricing. 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 advice 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 stability, 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 report, 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-assets: (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”. 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.”
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 level. 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 Depositaries 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.

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.
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

- Academic/research institution
- Business association
- Company/business organisation
- Consumer organisation
- EU citizen
- Environmental organisation
- Non-EU citizen
- Non-governmental organisation (NGO)
- Public authority
- Trade union
- Other

First name
Paul

Surname
Fox

Email (this won't be published)
paul.fox@finance-watch.org

Country of origin

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

- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Djibouti
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antigua and Barbuda</td>
<td>Eswatini</td>
<td>Mali</td>
<td>Seychelles</td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td>Ethiopia</td>
<td>Malta</td>
<td>Sierra Leone</td>
<td></td>
</tr>
<tr>
<td>Armenia</td>
<td>Falkland Islands</td>
<td>Marshall Islands</td>
<td>Singapore</td>
<td></td>
</tr>
<tr>
<td>Aruba</td>
<td>Faroe Islands</td>
<td>Martinique</td>
<td>Sint Maarten</td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td>Fiji</td>
<td>Mauritania</td>
<td>Slovakia</td>
<td></td>
</tr>
<tr>
<td>Austria</td>
<td>Finland</td>
<td>Mauritius</td>
<td>Slovenia</td>
<td></td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>France</td>
<td>Mayotte</td>
<td>Solomon Islands</td>
<td></td>
</tr>
<tr>
<td>Bahamas</td>
<td>French Guiana</td>
<td>Mexico</td>
<td>Somalia</td>
<td></td>
</tr>
<tr>
<td>Bahrain</td>
<td>French Polynesia</td>
<td>Micronesia</td>
<td>South Africa</td>
<td></td>
</tr>
<tr>
<td>Bangladesh</td>
<td>French Southern and Antarctic Lands</td>
<td>Moldova</td>
<td>South Georgia and the South Sandwich Islands</td>
<td></td>
</tr>
<tr>
<td>Barbados</td>
<td>Gabon</td>
<td>Monaco</td>
<td>South Korea</td>
<td></td>
</tr>
<tr>
<td>Belarus</td>
<td>Georgia</td>
<td>Mongolia</td>
<td>South Sudan</td>
<td></td>
</tr>
<tr>
<td>Belgium</td>
<td>Germany</td>
<td>Montenegro</td>
<td>Spain</td>
<td></td>
</tr>
<tr>
<td>Belize</td>
<td>Ghana</td>
<td>Montserrat</td>
<td>Sri Lanka</td>
<td></td>
</tr>
<tr>
<td>Benin</td>
<td>Gibraltar</td>
<td>Morocco</td>
<td>Sudan</td>
<td></td>
</tr>
<tr>
<td>Bermuda</td>
<td>Greece</td>
<td>Mozambique</td>
<td>Suriname</td>
<td></td>
</tr>
<tr>
<td>Bhutan</td>
<td>Greenland</td>
<td>Myanmar</td>
<td>Svalbard and Jan Mayen</td>
<td></td>
</tr>
<tr>
<td>Bolivia</td>
<td>Grenada</td>
<td>Namibia</td>
<td>Sweden</td>
<td></td>
</tr>
<tr>
<td>Bonaire Saint Eustatius and Saba</td>
<td>Guadeloupe</td>
<td>Nauru</td>
<td>Switzerland</td>
<td></td>
</tr>
<tr>
<td>Bosnia and Herzegovina</td>
<td>Guam</td>
<td>Nepal</td>
<td>Syria</td>
<td></td>
</tr>
<tr>
<td>Botswana</td>
<td>Guatemala</td>
<td>Netherlands</td>
<td>Taiwan</td>
<td></td>
</tr>
<tr>
<td>Bouvet Island</td>
<td>Guernsey</td>
<td>New Caledonia</td>
<td>Tajikistan</td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td>Guinea</td>
<td>New Zealand</td>
<td>Tanzania</td>
<td></td>
</tr>
<tr>
<td>British Indian Ocean Territory</td>
<td>Guinea-Bissau</td>
<td>Nicaragua</td>
<td>Thailand</td>
<td></td>
</tr>
<tr>
<td>British Virgin Islands</td>
<td>Guyana</td>
<td>Niger</td>
<td>The Gambia</td>
<td></td>
</tr>
<tr>
<td>Brunei</td>
<td>Haiti</td>
<td>Nigeria</td>
<td>Timor-Leste</td>
<td></td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Heard Island and McDonald Islands</td>
<td>Niue</td>
<td>Togo</td>
<td></td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>Honduras</td>
<td>Norfolk Island</td>
<td>Tokelau</td>
<td></td>
</tr>
<tr>
<td>Burundi</td>
<td>Hong Kong</td>
<td>Northern Mariana Islands</td>
<td>Tonga</td>
<td></td>
</tr>
<tr>
<td>Cambodia</td>
<td>Hungary</td>
<td>North Korea</td>
<td>Trinidad and Tobago</td>
<td></td>
</tr>
</tbody>
</table>
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
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
Finance Watch

• 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.

37943526882-24

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

Please specify your activity field(s) or sector(s):

Public interest NGO

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:
Public interest NGO

• 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’. In this public consultation, a crypto-asset is considered as “a digital asset that may depend on cryptography and exists on a distributed ledger”. This notion is therefore narrower than the notion of ‘digital asset’ that could cover the digital representation of other assets (such as scriptural money).

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

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

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.

We agree that this initiative should concentrate on seeking to find an appropriate regulatory framework for financial instruments in digital format and, in particular, for amending financial sector legislation to accommodate the adoption of distributed ledger technology (DLT) and cryptography. The term ‘digital assets’, as defined in this Consultation Document, is not specific to the financial sector and likely to encompass a range of legal issues that should be addressed in general, rather than sectoral legislation.

We are skeptical, however, that so-called ‘crypto assets’ require a stand-alone regulatory framework within financial sector legislation. We feel strongly that the adoption of DLT and cryptography for the creation of digital financial instruments (‘tokenisation’) is a generic process that could, in due course, result in many categories of well-established and extensively regulated instruments being converted into, and traded as digital ‘tokens’. A consistent, forward-looking regulatory approach should therefore aim at seamlessly integrating these new formats into the existing legal framework, rather than creating a parallel, stand-alone regulatory regime.

We would advise against the use of the term ‘crypto assets’ and would recommend the use of the term ‘tokens’ (see 8. below). We believe that the scope of this initiative should cover digital instruments that take the form of encrypted, and validated entries on a distributed ledger (‘tokens’) (formal scope) and whose principal function is that of a ‘financial instrument’ or ‘payment instrument’ (functional scope) (see 60. below).
Question 6. In your view, would it be useful to create a classification of crypto-assets at EU level?

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

6.1 If you think it would be useful to create a classification of crypto-assets at EU level, please indicate the best way to achieve this classification (non-legislative guidance, regulatory classification, a combination of both, ...).

Please explain your reasoning:

5000 character(s) maximum

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

We believe that the principal categories, and criteria for the classification of ‘crypto assets’ (or ‘tokens’) must be enshrined in law in order to restore and maintain legal certainty and consistency. In accordance with the principle of ‘substance over form’ transactions that take place in ‘tokenised’ form must not be treated differently from transactions with the same economic substance that are closed in other, ‘traditional’ ways. Relevant EU legislation needs to be expanded and adapted accordingly.

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.

‘Crypto-assets’ (or ‘tokens’) that would qualify as ‘payment instruments’ or ‘financial instruments’ by virtue of their functionality, i.e. the primary economic substance of the underlying transaction, should be regulated in the same way as their traditional, ‘non tokenised’ counterparts. This is, in our view, necessary to preserve legal certainty, maintain a ‘level playing field’ between different segments of the financial markets and ensure a consistently high level of protection for investors.

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.
We would advise against the use of the term “crypto-assets” and recommend the use of the generic term ‘token’ as a common point of departure. ‘Crypto assets’ are not necessarily assets in their own right but primarily instruments in digital form (‘tokens’) that document a contractual agreement, or represent a claim on an underlying asset. We agree with the ECB’s observation that “the use of DLT to record and transfer a range of financial and payment instruments (or their representation) in digital form is a future possibility that should not be mistaken for the issuance of new asset types” (ECB, Occasional Paper No. 230, August 2019).

We broadly agree with the Commission’s proposed classification of crypto-assets into three main categories: ‘payment tokens’, ‘investment tokens’ and ‘utility tokens’. We note that EU law already recognises the term ‘virtual currency’, which is defined by item 18 in Article 3 of Directive 2018/843/EU (AMLD 5). This definition comprises, in our view, two categories that should be considered separately (see below).

As discussed above (Q1.) we would prefer the use of the term ‘token’ for digital instruments that rely on cryptography and exist on a distributed ledger. In line with the ‘see-through’ principle we would suggest a general classification comprising four categories of ‘tokens’:

The first category, ‘payment tokens’, would comprise ‘tokens’ that represent a ‘payment instrument’ in accordance with item 14 in Article 4 of Directive 2015/2366/EU (PSD 2). This category should be defined restrictively and comprise only ‘tokens’ that either qualify as ‘electronic money’ – as defined by Directive 2009/110/EC (EMD 2) – or so-called ‘stablecoins’ that are pegged to one or more official (‘fiat’) currency/-ies at a fixed rate and backed in full with ‘funds’ – as defined by Article 4(2) of Directive 2015/2366/EU (PSD 2) – denominated in the reference currency/-ies. This definition corresponds largely to the concept of ‘tokenised funds’, which is the basis for the majority of ‘stablecoins’ in issue today. Other ‘stablecoins’ that do not fulfil these criteria, e.g. ‘collateralised stablecoins’, are more similar to debt securities (reliance on the creditworthiness of the issuer) or derivative instruments and should therefore be classified as ‘investment (or security) tokens’. This would also be the case for ‘stablecoins’ that are backed with government securities, as opposed to ‘funds’. In due course, so-called ‘central bank digital currencies’ (CBDCs) should also be considered as ‘payment tokens’.

For regulatory purposes we would recommend a) restricting the category of ‘payment tokens’ to ‘payment instruments’ in accordance with PSD 2 and b) aligning the concepts of ‘payment token’ and ‘e-money token’. The definition of ‘payment instruments’ in PSD 2 is quite wide and capable of accommodating the use of digital ‘tokens’. The definitions of ‘payment transaction’ and ‘funds’ in PSD 2, and of ‘electronic money’ in EMD 2 may need to be adapted in order to cover a broader variety of use cases, such as a limited set of ‘stablecoins’ that conform to the description set out above.

Directive 2018/843/EU (AMLD 5) defines the term ‘virtual currency’ as a ‘digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically’. We believe that this category should be sub-divided further to separate ‘virtual coin tokens’ that are created ex nihilo, e.g. based on an algorithmic process (‘proof of work’, ‘mining’), and rely solely on bilateral acceptance, from other ‘tokens’, such as ‘stablecoins’, that are attached to a legally established currency’. ‘Virtual coin tokens’, such as Bitcoin, are not currencies and do not meet the basic criteria of ‘money’ (medium of exchange, unit of account, store of value). Contrary to official currencies, they are not accepted as legal tender and are not backed by the ‘full faith and credit’ of the issuing institution(s)/government(s). They do not meet the definition of ‘funds’ under PSD 2 and are therefore not eligible for completing a ‘payment transaction’. Neither are they a ‘means of exchange’: even when accepted – voluntarily – by merchants in exchange for goods or services, prices for these goods or services are almost always denominated in official currency – due to the extreme volatility of (crypto-to-fiat) exchange rates. Hence a purchase of goods or services paid for in Bitcoin is usually preceded by a conversion of Bitcoin into official currency. We conclude that ‘virtual coin tokens’ are, essentially, speculative financial instruments without economic substance whose value is determined, exclusively, by supply and demand in the markets. [response continues in 8.2]
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.

[Response continued from 8.1] They should therefore not be viewed as a sub-set of ‘payment tokens’ because their payment function is limited, derivative and, in any event, secondary to their function as a speculative financial instrument. They should instead be considered as a particularly high-risk class of ‘investment tokens’.

The second category would comprise ‘investment (or security) tokens’, and cover, in the first instance, any ‘token’ that replicates a regulated ‘financial instrument’ as listed in Section C of Annex I of Directive 2014/65/EU (MiFID II). We note that certain terms in this list have not been defined in EU law so far and should be harmonised as a matter of priority (see 60. below). If a token incorporates features of different (financial and non-financial) transactions, it should be classified according to its prevailing function. This ‘functionality test’ should take into consideration both the supply side (the issuer or beneficiary) and the demand side (the investor or subscriber). Any token that represents an underlying transaction where a) the investor (or subscriber) is incentivised primarily by the promise of a financial reward (profit); or b) the principal objective of the issuer (or beneficiary) is to raise funds (e.g. for R&D or other corporate purposes) for themselves or a related party, as opposed to effecting the sale of a product or service, should be considered, by default, as an ‘investment token’. ‘Virtual coin tokens’ represent a special case as they are issued for free, i.e. without monetary consideration, and autonomously, in accordance to an algorithmic process.

We would argue that this category of ‘investment tokens’ should also cover most of the ‘tokens’ issued in recent years in so-called ‘Initial Coin Offerings’ (ICOs), which were often labelled, misleadingly, as ‘utility tokens’. In these cases funds were raised from investors, usually by start-up companies, in exchange for the future delivery of a yet-to-be-developed product or service. We do not agree that this type of transaction should be regarded as a ‘forward sale’ as it usually lacks the required characteristics, i.e. delivery of a product or service that conforms to agreed specifications at the agreed price on the agreed date. In the case of most ICOs at least one of these criteria cannot be with any degree of certainty at the time of the issue. Instead, ‘token’ holders – often retail investors – effectively ended up funding the operations of a start-up company, bearing all of its operational and financial risk, without adequate financial compensation or governance rights. While we recognise that issues of digital ‘tokens’ could indeed become a viable, and valuable, way of lowering the hurdle for early-stage companies to access funding we are insistent that mis-labeling corporate debt as ‘forward purchase agreements’ is not a viable alternative to a functioning market for early-stage venture capital and investor protection must not be compromised in the process. We are encouraged, in this respect, by the recent emergence of Initial Exchange Offerings (IEOs), which appear to mark a degree of convergence between ICOs, Security Token Offerings (STOs), and the traditional, formalised process of issuing securities.

The third category, ‘utility tokens’, would cover any ‘token’ that provides its holder with a right to obtain or access a specific product or service. In line with the ‘see-through’ principle we would argue that financial sector-specific regulation is appropriate, and necessary only if the economic substance of the underlying contract is primarily financial in nature. This should be true, a priori, for ‘payment tokens’, ‘investment tokens’ and ‘virtual currency tokens’. We would therefore propose, a contrario, that any ‘crypto asset’ that does not qualify as one of the preceding categories should be designated as a ‘utility token’ and should not be subject to financial sector regulation. They should, however, always be subject to mandatory registration with the relevant authorities and may well be subject to other relevant legislation, in particular related to consumer protection.

We do not see any need for defining a separate category of ‘hybrid tokens’. It is inherent in the process of
‘tokenisation’ that it allows for the combination of different features and functionalities. We believe, in the interest of legal clarity, that each ‘crypto asset’ (or ‘token’) should be assigned unequivocally to one of the regulatory categories discussed above, in accordance with its and prevailing function and economic substance. Issuers or sponsors would be responsible to determine, in the first instance, which category their ‘token’ would fall into. It would then be incumbent upon the relevant authorities to monitor issuance so as to ensure that ‘tokens’ issued on their markets are designated correctly.

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?**

According to Article 2(3) of Directive 2014/49/EU (DGSD) a ‘deposit’ is composed of ‘funds’, which, in turn, comprise “banknotes and coins, scriptural money or electronic money” (item 25 in Article 4(2) of Directive 2015/2366/EU (PSD 2). We would therefore argue that only ‘payment tokens’ that qualify as ‘e money’ (see 8. above) could qualify as a ‘deposit’. In the future, holdings of central bank-issued digital currency (CBDC) could qualify as a “deposit”.

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

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

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 can 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)

<table>
<thead>
<tr>
<th>Benefit</th>
<th>1 (not important at all)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (very important)</th>
<th>Don’t know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Issuance of utility tokens as an alternative funding source for start-ups</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Cheap, fast and swift payment instrument</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Enhanced financial inclusion</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Crypto-assets as a new investment opportunity for investors</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Improved transparency and traceability of transactions</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Enhanced innovation and competition</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Improved liquidity and tradability of tokenised ‘assets’</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Enhanced operational resilience (including cyber resilience)</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
<tr>
<td>Security and management of personal data</td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
<td><img src="image" alt="Rating" /></td>
</tr>
</tbody>
</table>
Possibility of using tokenisation to coordinate social innovation or decentralised governance

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.

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.

In accordance with our general views on the scope of this initiative (see 1. above) and the proposed categorisation of crypto-assets (or ‘tokens’) (see 8. above) we believe that the principal driver for the mainstream adoption of ‘crypto assets’ (or ‘tokens’) will be the ‘tokenisation’ of existing classes of ‘financial instruments’ and payment instruments’. The main benefits of ‘tokenisation’ are a) the inherent resilience of the distributed-ledger architecture; b) the transparency and traceability of transactions and holdings; and c) the potential to combine functionalities and automate certain processes, e.g. by way of ‘smart contracts’. While we expect a wide range of existing instruments to be replicated in ‘token’ form in due course we are very skeptical of ‘utility tokens’ as ‘an alternative funding source for start–ups’. This notion is at odds with the basic tenets of corporate finance, i.e. the concept of equity risk, and should not be entertained by the legislator.

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


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

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)

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

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 market for ‘crypto-assets’ has already seen its fair share of ill-advised, let alone fraudulent propositions and widespread use for money-laundering purposes. Estimates from different sources indicated that there have been more than 5,000 Initial Coin Offerings (ICOs) during the period from 2014 to 2019; as of March 2020, more than 1,000 of these issues have been abandoned, or exposed as fraud, and at least one-half is trading at prices close to zero or not at all. An estimated USD 30 billion, possibly more, were invested, often by retail investors. We believe that the lack of proper procedures governing the issuance and trading of these instruments, including adequate rules for the classification of instruments, disclosure requirements and regulated venues, have contributed significantly to exposing investors to undue risk and should be remedied promptly. In addition, ‘virtual coin tokens’ have become a popular route for criminal actors to convert and transfer illicit funds. More transparency and better supervision, in particular of exchanges where ‘virtual coin tokens’ are converted from, and into official (‘fiat’) currency will be necessary to stop these channels funding criminal activities.

We understand that the ‘proof of work’ process of validating transactions and ‘mining’ new ‘tokens’ in a public, permission-less DLT infrastructure, as is the case for the creation ‘virtual coin tokens’, can be extremely energy-intensive. A recent study by the University of Cambridge has estimated the annual energy consumption of the Bitcoin network to be equal to that of Switzerland. We do not believe that this economic model is either desirable nor sustainable and would expect that most DLT infrastructures will, in due course, move towards other validation/consensus mechanisms and/or permissioned models.

So far, the market for ‘crypto-assets’ (or ‘tokens’) is not substantial enough to pose a systemic risk. Given the expected rapid growth, and the potential arrival of large new entrants, such as Libra, the "stablecoin” sponsored by Facebook, it is conceivable that some segments of this market could pose systemic challenges unless adequate regulation is put in place in good time.

“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’ are crypto-assets whose value is anchored to real world ‘reference’ assets (e.g. cash and/or securities denominated in official currency/-ies, commodities, such as gold, or physical assets, such as property), and, in some instances, underpinned by a repurchase or redemption guarantee provided by the issuer.

When considering the legal and regulatory treatment of ‘stablecoins’ it is critical, in our view, not to lose track of the implicit logic of ‘tokenisation’, i.e. that ‘tokens’ are a digital representation of an underlying asset or contractual obligation – but not the reverse. To define ‘stablecoins’ as a new, stand-alone category of ‘crypto assets’ appears thoroughly misguided.

Depending on their design ‘stablecoins’ should, in our view, be classified as either ‘payment tokens’ (when used as a digital representation of ‘funds’, see 8. above) or ‘as investment tokens’ (when offered to the general public as ‘financial instruments’, e.g. as tokenised funds, collateralised or algorithmic stablecoins).

For illustration, Libra, the ‘stablecoin’ proposed by a consortium around Facebook, would be the ‘tokenised’ equivalent of a money market fund, with users of the ‘stablecoin’ effectively investing in a ‘reserve fund’, managed by the Libra Association, that consists of short term government debt securities. Libra ‘tokens’ should be classified as units in a collective investment fund, the Libra Reserve Fund, with the Libra Association as its regulated managing entity.

**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)

<table>
<thead>
<tr>
<th>Risk</th>
<th>1 (factor not relevant at all)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (very relevant factor)</th>
<th>Don’t know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraudulent activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Market integrity (e.g. price, volume manipulation...)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investor/consumer protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-money laundering and CFT issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data protection issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competition issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber security and operational risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

We would argue that the risk profile of ‘stablecoins’ depends on their design. ‘Stablecoins’ that qualify as ‘payment tokens’ (see 8. and 12 above) should, in principle; exhibit a lower risk profile than uncollateralised ‘tokens’. Nevertheless holders are exposed to potential fraud (by the issuer) or market abuse (by other market participants, e.g. operators of exchanges). Energy consumption is rated as a less critical issue here because we assume that these ‘tokens’ are issued, rather than ‘mined’ and likely to exist on a permissioned DLT infrastructure that does not rely on energy-intensive ‘proof of work’.

We could see financial stability as a material issue if the reserve fund of a ‘stablecoin’ is of such a size that it could potentially become a source of systemic risk.

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.

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)?
14.1 Please explain your reasoning for your answer to question 14:

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

We believe that ‘tokenisation’ is a generic process, triggered by advances in computing and cryptography, that will affect and transform certain segments of the financial sector, and indeed many other sectors, for some time. For the most part this process will affect the form, rather than the substance, of financial instruments and the way they are issued and traded. We recognise that ‘tokenisation’ introduces certain new elements into the financial ecosystem, such as the ‘token’ itself, ‘distributed ledgers’, ‘mining’ and ‘validation’ processes, and ‘smart contracts’. In the interest of continuity, consistency and legal certainty it is, in our view paramount to incorporate these new concepts into the existing legal and regulatory framework. We do not see any fundamental obstacles to adapting the existing legislation accordingly.

Question 15. What is your experience (if any) as regards national regimes on crypto-assets?

Please indicate which measures in these national laws are, in your view, an effective approach to crypto-assets regulation, which ones rather not.

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

N/A

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

Please indicate if such a bespoke regime should include the above-mentioned categories (payment, investment and utility tokens) or exclude some of them, given their specific features (e.g. utility tokens).
We do not subscribe to the implied assumption that inducing innovation and protecting users are contradictory objectives. Neither do we agree with the inherent assumption that innovation requires, or benefits from a lack of regulation. We would argue, much to the contrary, that well-considered and consistent regulation creates the legal certainty and predictability needed to encourage investment in long-term innovation. In keeping with the principle of ‘substance over form’ we believe that it is the responsibility of the legislator to ensure that ‘crypto assets’ (or ‘tokens’) that expose users to specific risks should be regulated in precisely the same way as ‘traditional’ instruments that exhibit the same risk profile.

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, ...):

As mentioned previously, we believe that EU legislation should be extended and adapted wherever necessary so that ‘tokens’ are regulated consistently and in accordance with the economic substance of the underlying transaction. Financial institutions’ exposures related to ‘tokenised’ payment and financial instruments should be accounted for, and disclosed in the same way as the corresponding ‘traditional’ instruments. Exposures to ‘virtual coin tokens’ – and derivative instruments based on these ‘tokens’ should be disclosed separately due to their high inherent risk.

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

Yes. This is especially important for so called ‘smart contracts’ which allow two or more individuals to enter into an agreement which is subsequently executed by code. Harmonisation of national civil law is likely to become critical to ensure a common approach, e.g. regarding the conditions for the legal transfer of title, liability, e.g. for non-performance, and enforcement.

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?

N/A

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.

So called ‘crypto assets’ (or ‘tokens’) are, by definition, immaterial, i.e. do not exist in physical form, and are issued and traded online. It is therefore difficult to reliably establish the jurisdiction which will be responsible for enforcing claims and protecting investors. It appears appropriate therefore to require issuers or sponsors who seek to offer ‘tokens’ to private investors and/or consumers in the EU to be established in the EU and to submit to the jurisdiction of an EU member state in respect of any legal claims arising in connection with the offer or the ‘token’

**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*
For ‘crypto-assets’ (or ‘tokens’) that qualify as ‘financial instruments’ or ‘payment instruments’ the corresponding regulatory requirements must apply. For instance, a new issue of an ‘investment token’ that replicates a debt or equity security should be accompanied by a prospectus that conforms with the requirements of Regulation 2017/1129/EU, with the issuer and sponsor accepting full legal responsibility for its content. A ‘token’ that represents a unit trust (UCITS)-like instrument should be a Key Investor Information Document (KIID) in accordance with Section 3 of Chapter IX Directive 2009/65/EC (UCITS IV).

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)

<table>
<thead>
<tr>
<th></th>
<th>1 (completely irrelevant)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (highly relevant)</th>
<th>Don’t know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Consumer Rights Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The E-Commerce Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The EU Distance Marketing of Consumer Financial Services Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

As mentioned previously (see 8. above), ‘payment tokens’ should conform, by definition with Directives 2015/2366/EU (PSD 2) and 2009/110/EC (EMD 2), as amended, and would be regulated there. We would recommend that ‘utility tokens’ – i.e. ‘tokens’ whose economic substance is not predominantly of a financial nature – should not be subject to financial-sector legislation but regulated in accordance with the economic substance of the underlying transaction. Legislation listed in this table may, or may not be applicable accordingly.
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.

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)

<table>
<thead>
<tr>
<th></th>
<th>1 (completely irrelevant)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (highly relevant)</th>
<th>Don’t know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>The managers of the issuer or sponsor should be subject to fitness and probity standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
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.

We do not see a need to distinguish between “stablecoins” and “global stablecoins” or, for that matter, for a definition of “stablecoins” as a separate category altogether. As mentioned previously (see 8. and 12. above), “stablecoins” should be considered as particular sub-sets of ‘payment tokens’ or ‘investment tokens’, depending on their design.

In respect of so-called ‘tokenised funds’, which represent the vast majority of ‘stablecoins’ in issue today, the ECB observes that “the tokenisation of funds denominated in any given currency does not constitute a new type of asset. It is rather an example of a traditional asset that uses DLT as its infrastructure and, on a case-by-case basis, may fall outside the scope of the regulatory framework that is applied to similar centralised initiatives or schemes while posing similar risks to the economy”. We agree with the ECB’s
assessment and the implied call for the legislator to restore regulatory consistency by amending the relevant legislation, such as PSD 2 and EMD 2.

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.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Relevant</th>
<th>Not relevant</th>
<th>Don't know / no opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The assets or funds of the reserve should be segregated from the issuer’s balance sheet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The assets of the reserve should not be encumbered (i.e. not pledged as collateral)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obligation for the assets or funds to be held in custody with credit institutions in the EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Periodic independent auditing of the assets or funds held in the reserve</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Relevant</th>
<th>Not relevant</th>
<th>Don’t know / no opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The assets or funds of the reserve should be segregated from the issuer's balance sheet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The assets of the reserve should not be encumbered (i.e. not pledged as collateral)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obligation for the assets or funds to be held in custody with credit institutions in the EU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obligation for the assets or funds to be held for safekeeping at the central bank</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Periodic independent auditing of the assets or funds held in the reserve</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obligation for the issuer to use open source standards to promote competition</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

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.

The criteria set out above describe, in our view, a type of ‘stablecoin’ that is also known as ‘tokenised funds’, except that it appears to include short-term government securities as part of the reserve fund. We refer to our reasoning in respect of questions 8. and 12. above. ‘Stablecoins that represent an investment in securities, i.e. effectively replicate a collective investment vehicle, should conform with all relevant provisions of Directives 2009/65/EC (UCITS IV) or Directive 2011/61/EU (AIFMD), as applicable.

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.

<table>
<thead>
<tr>
<th>Description</th>
<th>Relevant</th>
<th>Not relevant</th>
<th>Don’t know / no opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)</td>
<td>![Relevant]</td>
<td>![Not relevant]</td>
<td>![Don’t know / no opinion]</td>
</tr>
<tr>
<td>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</td>
<td>![Relevant]</td>
<td>![Not relevant]</td>
<td>![Don’t know / no opinion]</td>
</tr>
<tr>
<td>The assets or funds of the reserve should be segregated from the issuer’s balance sheet</td>
<td>![Relevant]</td>
<td>![Not relevant]</td>
<td>![Don’t know / no opinion]</td>
</tr>
<tr>
<td>The assets of the reserve should not be encumbered (i.e. not pledged as collateral)</td>
<td>![Relevant]</td>
<td>![Not relevant]</td>
<td>![Don’t know / no opinion]</td>
</tr>
</tbody>
</table>
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)

The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating

Obligation for the assets or funds to be held in custody with credit institutions in the EU

Periodic independent auditing of the assets or funds held in the reserve

The issuer should disclose information to the users on (i) how it intends to provide stability to the “stablecoins”, (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve

The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically

25.2 a) Is there any other requirements not mentioned above that could be imposed on “stablecoins” issuers and/or the manager of the reserve? Please specify which one(s) and explain your reasoning:

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

25.2 b) Please illustrate your responses to question 25.2:

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

See response to question 25.1. above.

“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”.

32
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.

As mentioned previously, we do not see a need to differentiate between different categories of ‘stablecoins’. To the extent that ‘stablecoins’ qualify as ‘payment tokens’, certain wholesale applications may, for instance, fall under the exclusions already provided by items (h) (i), (m) or (n) of Article 3 of Directive 2015/2366/EU (PSD 2). For ‘stablecoins’ that qualify as ‘investment tokens’ we would make reference, for instance, to the requirement in Directive 2014/65/EU (MiFID II) to assess the suitability of certain financial instruments for particular clients, in particular retail investors.

2. Trading platforms

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

.................................................................................................................................................................................................................................................................................. ¹⁹

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)
<table>
<thead>
<tr>
<th>Risk</th>
<th>Not Relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absence of accountable entity in the EU</td>
<td></td>
</tr>
<tr>
<td>Lack of adequate governance arrangements, including operational</td>
<td></td>
</tr>
<tr>
<td>resilience and ICT security</td>
<td></td>
</tr>
<tr>
<td>Absence or inadequate segregation of assets held on the behalf of</td>
<td></td>
</tr>
<tr>
<td>clients (e.g. for ‘centralised platforms’)</td>
<td></td>
</tr>
<tr>
<td>Conflicts of interest arising from other activities</td>
<td></td>
</tr>
<tr>
<td>Absence/inadequate recordkeeping of transactions</td>
<td></td>
</tr>
<tr>
<td>Absence/inadequate complaints or redress procedures are in place</td>
<td></td>
</tr>
<tr>
<td>Bankruptcy of the trading platform</td>
<td></td>
</tr>
<tr>
<td>Absence/inadequate complaints or redress procedures are in place</td>
<td></td>
</tr>
<tr>
<td>Lacks of resources to effectively conduct its activities</td>
<td></td>
</tr>
<tr>
<td>Losses of users’ crypto-assets through theft or hacking (cyber risks)</td>
<td></td>
</tr>
<tr>
<td>Lack of procedures to ensure fair and orderly trading</td>
<td></td>
</tr>
<tr>
<td>Access to the trading platform is not provided in an undiscriminat-</td>
<td></td>
</tr>
<tr>
<td>ing way</td>
<td></td>
</tr>
<tr>
<td>Delays in the processing of transactions</td>
<td></td>
</tr>
<tr>
<td>For centralised platforms: Transaction settlement happens in the</td>
<td></td>
</tr>
<tr>
<td>book of the platform and not necessarily recorded on DLT. In those</td>
<td></td>
</tr>
<tr>
<td>cases, confirmation that the transfer of ownership is complete lies</td>
<td></td>
</tr>
<tr>
<td>with the platform only (counterparty risk for investors vis-à-vis the</td>
<td></td>
</tr>
<tr>
<td>platform)</td>
<td></td>
</tr>
<tr>
<td>Lack of rules, surveillance and enforcement mechanisms to deter</td>
<td></td>
</tr>
<tr>
<td>potential market abuse</td>
<td></td>
</tr>
</tbody>
</table>

**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*
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)

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

### 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.

We would expect trading of ‘crypto-assets’ (‘tokens’) to take place on platforms that are either Regulated Markets (RMs), Multi-Lateral Trading Facilities (MTFs) or Organised Trading Facilities (OTFs) and therefore conform to the respective regulatory requirements.

### 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)

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>1 (completely irrelevant)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (highly relevant)</th>
<th>Don’t know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absence of accountable entity in the EU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of adequate governance arrangements, including operational resilience and ICT security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conflicts of interest arising from other activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Absence/inadequate recordkeeping of transactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Absence/inadequate complaints or redress procedures are in place</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bankruptcy of the exchange</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadequate own funds to repay the consumers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Losses of users’ crypto-assets through theft or hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users suffer loss when the exchange they interact with does not exchange crypto-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>1 (completely irrelevant)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (highly relevant)</th>
<th>Don’t know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absence of accountable entity in the EU</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>
Exchanges should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)

Exchanges should segregate the assets of users from those held on own account

Exchanges should be subject to rules on conflicts of interest

Exchanges should be required to keep appropriate records of users’ transactions

Exchanges should have an adequate complaints handling and redress procedures

Exchanges should be subject to prudential requirements (including capital requirements)

Exchanges should be subject to advertising rules to avoid misleading marketing/promotions

Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)

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

30.1 Is there any other requirement that could be imposed on 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.
4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys and to interact with DLT to allow users to send and receive crypto-assets and monitor their balances. Crypto-asset wallets come in different forms. Some support multiple crypto-assets/DLTs while others are crypto-asset/DLT specific. DLT networks generally provide their own wallet functions (e.g. Bitcoin or Ether).

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

---

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)

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>1 (completely irrelevant)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (highly relevant)</th>
<th>Don’t know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>No physical presence in the EU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of adequate governance arrangements, including operational resilience and ICT security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Absence or inadequate segregation of assets held on the behalf of clients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conflicts of interest arising from other activities (trading, exchange)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abnormal/inadequate recordkeeping of holdings and transactions made on behalf of users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Absence/inadequate complaints or redress procedures are in place</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bankruptcy of the custodial wallet provider</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inadequate own funds to repay the consumers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The custodial wallet is compromised or fails to provide expected functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The custodial wallet provider behaves negligently or fraudulently</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No contractual binding terms and provisions with the user who holds the wallet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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)

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

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:
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:

Based on the principle of ‘substance over form’ services offered by wallet providers are identical in substance to custodial and depositary services that are defined as ‘ancillary services’ in in Section B of Annex I of Directive 2014/65/EU (MiFID II) and should be regulated accordingly.

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:

Authorisation for custodial wallet providers should be aligned with the type of regulated business they are authorised to transact. In respect of ‘security tokens’ the operation of a custodial wallet is without doubt functionally equivalent to the operation of a securities deposit, which is an ‘ancillary service’ within the meaning of item 1 in Section B of Annex I of Directive 2014/65/EU (MiFID II). Whereas most securities deposits are operated electronically already today there may be specific requirements in respect of the safekeeping and administration of ‘tokenised’ securities that would have to be take into account by amending the legislation in force. This approach would be applicable, by analogy, to other relevant legislation, such as Directive 2009/65/EC (UCITS IV).
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?

The scope of this initiative should be limited, in our view, to financial instruments and services. Relevant legislation, such as Directive 2014/65/EU (MiFID II), should therefore be applicable.

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)

<table>
<thead>
<tr>
<th>1 (completely irrelevant)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (highly relevant)</th>
<th>Don't know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Reception and transmission of orders in relation to crypto-assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution of orders on crypto-assets on behalf of clients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crypto-assets portfolio management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advice on the acquisition of crypto-assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Underwriting of crypto-assets on a firm commitment basis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Placing crypto-assets on a firm commitment basis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Placing crypto-assets without a firm commitment basis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Services provided by developers that are responsible for maintaining/updating the underlying protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

The upper section of the above table mirrors the list of ‘investment services’ in Section A of Annex I of Directive 2014/65/EU (MiFID II). The risks of leaving these services unregulated for ‘tokenised’ financial instruments are essentially the same that justify regulation of their ‘traditional’ counterparts under MiFID II.

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

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

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

36.1 Please explain your reasoning for your answer to question 36:

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

As mentioned previously (8. and 12. above) we would recommend expanding the scope of PSD 2 and ESD 2 to include certain categories of so called ‘stablecoins’ that qualify, in our view, as ‘payment tokens’. These would include, in particular, ‘tokens’ that are pegged to one or more official currency/-ies and fully supported by cash balances in these currencies (‘tokenised funds’).

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)

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

**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.

**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.

Supervision of ‘crypto–assets’ (or ‘tokens’), and relevant service providers, should be part of the regulatory remit of competent authorities, both at the EU and member state level. Issuance and trading of ‘crypto–assets’, with the exception of ‘utility tokens’ (see 8. above), should be transitioned to regulated markets, such as RMIs, MTFs and OTFs, and handled by regulated market participants. Supervisors will need to acquire relevant competencies and build capacity to effectively monitor the market and detect market integrity issues in a timely manner. Adequate enforcement mechanisms will have to be put into place to deter and/or sanction misconduct.

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 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.

Trading in ‘crypto–assets’ (or ‘tokens’) should be subject to the same requirements as trading in ‘traditional’ financial instruments. Upon opening a client account (electronic wallet) investors should be required to produce official identification, e.g. in conformity with Regulation 910/2014/EU (eIDAS). The same principle
should apply for accounts holding ‘payment tokens’.

We are mindful that a balance needs to be struck between the need to ensure that ownership of wallets is properly assigned, which is necessary, in particular, to protect counterparties and prevent money-laundering, and the right of wallet holders to see their privacy respected. It is, however, entirely feasible for the wallet holder’s identity to be known to the wallet provider but anonymised towards third parties.

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.

We recognise the risk that the EU legislative framework does not prevent EU citizens or entities from trading ‘crypto–assets’ or ‘tokens’ on third-country exchanges. We would argue, however, that the risk of circumvention, as well as regulatory arbitrage, is not unique to the ‘crypto–assets’ sphere but fairly common in a largely globalised financial market. The most effective protection against circumvention, in our view, would be to maximise incentives for EU citizens and entities to conduct their business onshore. On the demand side, investors should be made aware that they would be engaging with non–EU service providers at their own risk and foregoing the benefits of investor protection under EU law. The more favourably EU investor protection compares vis à vis third countries the less inclined EU investors will be to expose themselves to higher risk. On the supply side, circumvention, and regulatory arbitrage could be mitigated by banning service providers who are not registered and regulated in the EU, or in a jurisdiction that applies a regulatory regime of equivalent quality, from offering regulated services to EU citizens and entities.

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.

The scope of this initiative should be limited, in our view, to financial instruments and the categorisation we propose would not necessitate the use of the proposed terms and concepts. As mentioned previously (see 5. above) we believe that a bespoke regulatory regime for ‘crypto assets’ is not appropriate.

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

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

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

42.1 Please explain your reasoning for your answer to question 42:

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

Criminal actors are well versed in identifying weak links that allow them to introduce illicit funds into the financial system. To preserve the integrity of the system it is critical to ensure that all potential entry points are adequately protected and market participants are held legally responsible.

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.

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
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)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Don’t know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Service providers must be able to demonstrate their ability to have all the controls in place in order to be able to</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
46.1 Please explain your reasoning for your answer to question 46:

We note that these obligations are in place already today for most actors in the EU financial markets, including even very small, advisory-only firms. We do not see any compelling reason for exempting the ‘crypto-assets’ segment, which is, in anything, even more susceptible to AML/CFT risks.

3. Consumer/investor protection

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

---

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.


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)
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.

47.2 Please explain your reasoning for your answer to question 47 and indicate if those requirements should apply to all types of crypto assets or only to some of them:

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

The appropriate requirements may differ for each class of ‘crypto-assets’ (or ‘tokens’). Requirements for ‘investment tokens’ should mirror the requirements for the underlying financial instrument, i.e. a securities prospectus or, in the case of a UCITS-type structure, a Key Investor Information Document (KIID).

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.

In keeping with our general argument that most ‘crypto–assets’ are ‘tokenised’ representations of financial or payment instruments we would suggest that the standards of consumer protection that are deemed appropriate in respect of the underlying ‘traditional’ instruments should, as a general rule, also apply to their digital versions.

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.

The distinction between ‘public’ and ‘private’ offers may be less useful in the context of placements that are conducted online. We recognise the need for a degree of proportionality in regulating such offers but would suggest that the risk profile of the instrument (‘token’), the size (amount) of the issue and the number of subscribers may be more useful criteria for assessing the appropriate level of investor protection required. Rules for simplified requirements already exist in various relevant pieces of legislation, e.g. the ‘growth prospectus’ in accordance with Article 15 of Regulation 2017/1129/EU.

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
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)

<table>
<thead>
<tr>
<th></th>
<th>1 (factor not relevant at all)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (very relevant factor)</th>
<th>Don't know / no opinion / not relevant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Those crypto-assets should be banned</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Those crypto-assets should be still accessible to EU consumers/investors</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>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</td>
<td>o</td>
<td></td>
<td></td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>

**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.
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.

An outright ban on such ‘crypto–assets (or ‘tokens’) does not appear practically feasible and may well be counter–productive. It may be preferable for such instruments to be traded in the EU, with trading subject to EU regulation, if EU investors would otherwise trade them on a non–EU market. It should be clear, however, that these instruments are not covered by EU investor protection rights and we would suggest restricting access to such instruments to professional investors, on the assumption that they are more versed in assessing risk and aware of the implications of foregoing EU investor protection. It may still be appropriate, nonetheless, to exclude certain instruments from trading in exceptional cases. Such a ban should be imposed only on a case-by-case basis if a particular instrument is found to carry unusual risks that are outside the legally acceptable boundaries.

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
Providers who offer services in more than one EU jurisdiction should, a priori, be subject to supervisory coordination or supervision at the EU level, as appropriate. Whether or not supervision should be exercised at the EU level should be determined based on the ongoing monitoring and assessment of a) the potential systemic risk posed and/or b) a dominant market position being held by any actor or group of actors.

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.

N/A

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

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

A. General questions on ‘security tokens’

Introduction

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

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

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

Current trends concerning security tokens

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

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

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

The Commission services’ understanding is that permissionless networks and decentralised platforms\(^29\) are still in their infancy, with uncertain prospects for future applications in financial services due to their higher trade latency and lower liquidity. Permissionless decentralised platforms could potentially develop only at a longer time horizon when further maturing of the technology would provide solutions for a more efficient trading architecture. Therefore, it could be premature at this point in time to make any structural changes to the EU regulatory framework.
Security tokens are, in principle, covered by the EU legal framework on asset management in so far as such security tokens fall within the scope of “financial instrument” under MiFID II. To date, however, the examples of the regulatory use cases of DLT in the asset management domain have been incidental.

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

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

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

26 See section IV.2.5 for further information

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

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

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

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

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

| N/A |

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
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.

We are aware of a number of initiatives within the industry that look at using DLT to improve pre- and post-trade transparency – by providing real-time information on holders of securities and units – and to facilitate post-trade settlement. We believe that the benefits of DLT-based applications could be particularly relevant in these areas. We understand that many of these use cases are still facing technical constraints, e.g. regarding processing speed and throughput, that still need to be addressed and may delay the widespread adoption of DLT.

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.

We expect that DLT-based technology will be adopted in due course by most market participants including established providers of securities trading and management services. It is likely, in our view, that the
migration to this new technology platform will occur gradually. Given the already very concentrated structure of this market and the conservative attitude of its customer base we do not expect this technological transition to alter the structure of this marketplace or challenge the position of incumbents in a way that could materially affect financial stability.

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.

See answer to question 56. above.

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

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

58.1 Please explain your reasoning for your answer to question 58:

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

We agree that regulation should first be aimed at covering permissioned, centralised infrastructure, which we expect to be deployed by major incumbent operators. We would suggest that regulators and supervisors should monitor the development of alternative, decentralised structures, in particular those based on permission-less DLT, and be ready to extend the regulatory scope accordingly, as and when appropriate.
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
As mentioned previously (see 8. above) we are proposing an approach which puts ‘substance over form’ and starts from the assumption that any ‘token’ whose primary function is that of a ‘financial instrument’ should be classified as an ‘investment token’. ‘Security tokens’ would be a sub-set of ‘investment tokens’ that fulfil the criteria of a (transferable) security and would therefore always be ‘financial instruments’ according to our reasoning. We are mindful that Section C of Annex I of Directive 2014/65/EU (MiFID II) does not provide a definition of ‘transferable security’ and that the meaning of this term is interpreted differently between EU member states. We believe, however, that a common legal definition of this term is long overdue and would strongly support a legislative effort to arrive at such a definition.

**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)

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

**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.

As mentioned above (see 59.) we believe that the absence of common definitions for various categories of ‘financial instruments’ listed Section C of Annex I of Directive 2014/65/EU (MiFID II) – including, but not limited to the term ‘transferable securities’ – is a major source of legal inconsistency and uncertainty, and a fundamental obstacle on the way towards a Capital Markets Union. We would therefore welcome a legislative initiative that harmonises these terms at the EU level. This would also provide a stable basis for anchoring the corresponding definitions of digital ‘tokens’ and go a long way towards creating a unified, consistent regulatory framework for ‘traditional’ and digital financial instruments.

**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)

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

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.
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.

As mentioned above (see 8.) we would argue that 'tokens' should be classified according to their prevailing function. If the function is primarily financial, either from the issuer's or from the subscriber's perspective, the 'token' should be considered as an 'investment token' and regulated accordingly. This does not rule out, however, that the 'its secondary, non-financial functions could be subject to another set of laws and regulations.

One example could be the proposed treatment of 'tokens' that promise the holder delivery of a yet-to-be-developed product or service in the future in return for funding a start-up company. We believe that such an agreement should be classified as a financial instrument because its primary objective, from the perspective of the issuer, is to obtain funding. The subscriber agrees to take delivery of the promised good or service in lieu of claiming repayment of the loaned amount (and interest). While the 'loan' part of the transaction is financial, the supply of a physical good or service, would be governed by a different set of rules.

1.2. Investment firms

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

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

- [ ] Completely agree
- [ ] Rather agree
- [ ] Neutral
- [ ] Rather disagree
- [ ] Completely disagree
- [ ] Don’t know / no opinion / not relevant

62.1 Please explain your reasoning for your answer to question 62:

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

We believe that the existing framework can be applied with some modifications (see 8. and 60. above). These modifications should be made by way of amending the relevant legislation and, where necessary, issuing detailed guidance by way of delegated and implementing acts.
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.

See answer to question 62. above.

1.3 Investment services and activities

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

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

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

64.1 Please explain your reasoning for your answer to question 64:

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

The list of ‘investment services’ and ‘ancillary services’ in Sections A and B of Annex I may need to be amended to take into account certain activities that are specific to ‘crypto–assets (or ‘tokens’), such as the
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.

N/A

1.4. Trading venues

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

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

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

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

5000 character(s) maximum
The existing definitions and requirements are likely to be applicable for most MTFs and OTFs that are already emerging as the primary venues for trading ‘crypto–assets’ (or ‘tokens’). It remains to be seen whether matching services that do not provide the convenience and reliability of simultaneous execution will manage to attract and sustain significant volumes of trading or whether their will remain marginal, rather like ‘traditional’ ‘bulletin boards’.

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.

We believe that existing formats and procedures are largely adequate and transferable. The mandatory content of information documents, such as prospectuses and KIIDs, may need to be amended to take into account the technical and legal specifics of ‘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.

It may be appropriate to provide for protective devices that are adapted particularly for online investment in ‘security tokens’, such as mandatory information screens and, potentially a ‘cooling off’ mechanism for...
certain high-risk instruments.

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.

In line with our general approach, which would see ‘security tokens’ covered by MiFID II by default, we would expect MiFID II investor protection to be extended to ‘security tokens’ as a matter of course.

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, it appears that DLT could be particularly suitable for market segments with limited trading volumes and low order frequencies that do not require high throughput. The transparency and traceability afforded, in
principle, by DLT could be of particular relevance for the SME segment, where equity interests are often closely held and any changes in the shareholder structure may have a material and immediate effect on the entity’s governance. The enhanced functionality of ‘tokens’ could also be used to implement typical features, such as selling restrictions and ‘lock up periods’.

1.7. Systems resilience, circuit breakers and electronic trading

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

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

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

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.

---

**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.

---
1.10 Pre and post-transparency requirements

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

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

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

- [ ] Completely agree
- [ ] Rather agree
- [ ] Neutral
- [ ] Rather disagree
- [ ] Completely disagree
- [ ] Don’t know / no opinion / not relevant

74.1 Please explain your reasoning for your answer to question 74:

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

We understand the difficulties to set transparency requirements in an emerging market where trading in most instruments is still rather thin. Adequate transparency is, however, a precondition for stimulating trading and encouraging investors to the market. It may be desirable therefore to consider adapting existing rules – for this segment only – and to adjust the calibration of requirements gradually as the market develops.

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.

See answer to question 74. above.
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.

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.

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.
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.

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)

<table>
<thead>
<tr>
<th></th>
<th>1 (not a concern)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (strong concern)</th>
<th>Don’t know / no opinion / strong concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency for significant net short positions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restrictions on uncovered short selling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competent authorities’ power to apply temporary restrictions to short selling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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.

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.
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.
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

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.
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.

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 could see a strong case, based on proportionality, to apply a simplified regulatory regime, such as the ‘growth prospectus’ to issues of ‘security tokens’ provided that the issuer is an SME and fulfils the criteria set out in Article 15 of Regulation 2017/1129/EU (see 49. above).

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.

Yes. The fact that ‘tokens’ exist only in digital, encrypted form and that their fungibility relies on the integrity of the relevant digital infrastructure (custodial wallet, ledger, verification) poses a variety of risks that are specific to this type of instrument and should be communicated to investors accordingly.

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?
<table>
<thead>
<tr>
<th></th>
<th>1 (not a concern)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (strong concern)</th>
<th>Don’t know / no opinion / strong concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition of ‘securities settlement system’ and whether a DLT platform can be qualified as securities settlement system under the SFD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition of ‘book-entry form’ and ‘dematerialised form’</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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);</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What could constitute delivery versus payment in a DLT network, considering that the cash leg is not processed in the network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What entity could qualify as a settlement internaliser</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

---

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.

---

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.
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)

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

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)

<table>
<thead>
<tr>
<th>Definition of a securities settlement system</th>
<th>1 (not a concern)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (strong concern)</th>
<th>Don’t know / no opinion / strong concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition of system operator</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Definition of participant</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Definition of institution</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Definition of transfer order</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>What could constitute a settlement account</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>What could constitute collateral security</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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.
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 ledger.  

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)

<table>
<thead>
<tr>
<th></th>
<th>1 (not a concern)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (strong concern)</th>
<th>Don't know / no opinion / strong concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>If crypto-assets qualify as assets that can be subject to financial collateral arrangements as defined in the FCD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 network? 

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

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)

<table>
<thead>
<tr>
<th>Issue</th>
<th>1 (not a concern)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (strong concern)</th>
<th>Don't know / no opinion / strong concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules on margin requirements, collateral requirements and requirements regarding the CCP’s investment policy</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Rules on settlement</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Organisational requirements for CCPs and for TRs</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Rules on segregation and portability of clearing members’ and clients’ assets and positions</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Rules on requirements for participation</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Reporting requirements</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

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
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.

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.

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)

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

<table>
<thead>
<tr>
<th>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;</th>
<th>1 (not suited)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (very suited)</th>
<th>Don't know / no opinion / very suited</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.


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

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

For instance, under the UCITS Directive, an investment company and a management company (for each of the common funds that it manages) shall ensure that a single depositary is appointed. The assets of the UCITS shall be entrusted to the depositary for safekeeping. For crypto-assets that are not ‘security tokens’ (those which do not qualify as financial instruments), the rules for ‘other assets’ apply under the UCITS Directive. In such a case, the depositary needs to ensure the safekeeping (which involves verification of ownership and up-to-date recordkeeping) but not the custody. This function could arguably cause perceived uncertainty where such assets are security tokens.

**Question 107. Do the provisions of the EU UCITS Directive legal framework in the following areas are appropriately suited for the effective functioning of DLT solutions and the use of security tokens?**

Please rate from 1 (not suited) to 5 (very suited)

<table>
<thead>
<tr>
<th>Provisions of the UCITS Directive pertaining to the eligibility of assets, including cases where such provisions are applied in conjunction with the notion &quot;financial instrument&quot; and/or &quot;transferable security&quot;</th>
<th>1 (not suited)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (very suited)</th>
<th>Don’t know / no opinion / very suited</th>
</tr>
</thead>
<tbody>
<tr>
<td>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;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCITS Directive rules on the arrangements for the identification, management and monitoring of the conflicts of interest, including between the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


management company and its clients, between two of its clients, between one of its clients and a UCITS, or between two -UCITS;

| UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens; |
| Disclosure and reporting requirements set out in the UCITS Directive. |

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?
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.

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.

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
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.

See answer to question 8. above.

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)

<table>
<thead>
<tr>
<th></th>
<th>1 (completely inappropriate)</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5 (completely appropriate)</th>
<th>Don't know / no opinion / very suited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial capital and ongoing funds</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Safeguarding requirements</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Issuance</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Redeemability</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Use of agents</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Out of court complaint and redress procedures</td>
<td>○</td>
<td></td>
<td></td>
<td></td>
<td>○</td>
<td></td>
</tr>
</tbody>
</table>

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.

See answers to questions 8. and 12. above.
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.

We believe that the framework is generally applicable for certain categories of ‘stablecoins’ that (see 8. and 12. above). We do not suggest to differentiate between ‘global’ and other ‘stablecoins’.

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

Specific privacy statement (https://ec.europa.eu/info/law/better-regulation/specifc-privacy-statement_en)

Contact

fisma-crypto-assets@ec.europa.eu