BNP PARIBAS

EU Transparency Register Identification Number: 78787381113-69

March 2020

EC CONSULTATION ON AN EU FRAMEWORK FOR MARKETS IN CRYPTO-ASSETS

General Comments

BNP Paribas Group would like to thank the European Commission (EC) for the opportunity to provide its views on an EU framework for markets in crypto-assets. Considering that **crypto-assets could have very important implications for the banking and financial sector in terms of potential opportunities and benefits as well as in terms of new risks related, for example, to financial stability, monetary policy or fight against money laundering and financing of terrorist activities**, we consider this consultation as an important step in the collective thinking to be conducted in this area and are pleased to provide our preliminary considerations.

In general terms, **we welcome the Commission's wish to develop a clear legal framework for crypto-assets.** Future EU rules will have to provide stakeholders with the legal certainty they need for the development of crypto-assets related activities. In this respect, these EU rules will have to **strike the right balance between the search for innovation and the protection of consumers and investors**. The adoption of a European regulatory framework should also contribute to **EU attractiveness** and strengthen its **capacity to influence international standards** in this area. **However, given the fact that both the various types of crypto-assets and the corresponding markets are not stabilized yet, temporary regulatory frameworks might be useful to allow experiments with a sufficient level of flexibility.**

As suggested by the European Commission, **we deem it necessary to develop a European classification of the various types of crypto-assets**. Indeed, such a classification would make it possible to define rules adapted to each of the different categories of assets thus defined. The classification, which should be set at the European level, could be based primarily on the crypto-asset's economic function. This European taxonomy should follow the "**same business, same risks, same rules, same supervision**" principle. In other terms, if the economic function and purpose of a crypto-asset are the same as a regulated asset class, it should be subject to the same set of financial and prudential rules. Moreover, any entity or intermediary engaging in crypto-assets activities that are equivalent to those performed by regulated financial entities or intermediaries, should be subject to the same legal requirements (in particular with respect to prudential and anti-money laundering issues). To date, the taxonomy proposed by the EC, which distinguishes between "payment", "investment", "utility" and "hybrid" tokens, seems relevant, and consistent with the state of the art. These different categories seem broad enough to cover all current cases of use and could be used to define the main legislative principles at level 1, while technical aspects and potential sub-categories of crypto-assets could be addressed by the European supervisory authorities (ESAs) at the second level.

Beyond this classification, **as regards "regulated" crypto-assets, i.e. those that qualify as "financial instruments" under MiFID II and those qualifying as "e- money" under EMD2, we consider that an adaptation of existing regulations – MiFID, EMIR, CESDR, etc.- would be the right approach, whereas, as regards non-regulated assets, i.e. all the crypto-assets that are not regulated at EU level, the principle of a new bespoke regime, as proposed by the Commission, seems to be necessary**. In any case, given that the environment of the crypto-assets

is still immature and that the necessary perspective and feedback that could allow to design fully appropriate rules are not yet available, we believe that it would be extremely useful to set up as soon as possible a European framework allowing experiments, under the supervision of the ESAs.

Stablecoins are also a core issue, given their potential impacts for monetary policy transmission and financial stability. **In this respect, we believe that only a CBDC (central bank digital currency) or a commercial bank digital currency, since they are different forms of a genuine money, can fully perform the functions of money : store of value, means of payment and unit of account**. However, it seems that the impact the CBDC could have both in terms of financial stability (risk of "digital" bank run) and on the monetary policy transmission (cost and volume of bank lending and money creation) should be carefully monitored. Moreover, as regards the financial markets, **in order to carry out end-to-end transactions with "tokenised" assets on the blockchain, financial institutions need a liquid and safe asset for making settlements. A detailed analysis should be conducted to assess whether a CBDC and/or a European wholesale ledger for commercial bank digital currencies, that would be convertible at parity with the euro[*], would be the best solution to satisfy this need**. Commercial bank digital currencies could be an effective way to allow the circulation of money on a blockchain and make a perfectly safe and liquid payment instrument available on it without jeopardizing the current framework of monetary policy which has very much proved its worth. **In any case, the development of an "e-euro", whether CBDC and/or commercial bank digital currency, would significantly help blockchain-based financial services to scale up and would also enhance the attractiveness and international role of the euro**.

Among the important topics is also the question of the conservation of security tokens. Indeed, we believe that **a clarification of the legal framework applicable to the conservation of security tokens by depositaries and their duty of restitution**, provided, in some cases by the UCITS and AIFM Directives, will be necessary in order to provide sufficient legal certainty for this activity.

[*] Such a ledger - which could be named "e-euro" -, accessible only to financial intermediaries, could help for the unlocking of the full potential of the blockchain technology.

Contribution ID: 073a44ed-11a7-4a0f-a6c8-327aebb26e20
Date: 19/03/2020 19:40:39

Public consultation an EU framework for markets in crypto-assets

Fields marked with * are mandatory.

Introduction

This consultation is also available in German and French.

Background for this public consultation

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

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

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

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

Crypto-assets are one of the major applications of blockchain for finance. Crypto-assets are commonly defined as a type of private assets that depend primarily on cryptography and distributed ledger technology as part of their inherent value[2]. 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[3]. There are many ways to classify the different types of crypto

assets[4]. 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[5]. 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[6] 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[7], 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[8], 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[9]: (i) For crypto-assets that are covered by EU rules by virtue of qualifying as financial instruments under the Markets in financial instruments Directive – MiFID II – or as electronic money/e-money under the Electronic Money Directive – EMD2 – the Commission services have screened EU legislation to assess whether it can be effectively applied. For crypto-assets that are currently not covered by the EU legislation, the Commission services are considering a possible proportionate common regulatory approach at EU level to address, inter alia, potential consumer/investor protection and market integrity concerns.

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

Responding to this consultation and follow up to the consultation

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

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

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

- **The second section seeks feedback from stakeholders on whether and how to classify crypto-assets**. This section concerns both crypto-assets that fall under existing EU legislation (those that qualify as 'financial instruments' under MiFID II and those qualifying as 'e-money' under EMD2) and those that do not.
- **The third section invites views on the latter, i.e. crypto-assets that currently fall outside the scope of the EU financial services legislation. In that first section, the term 'crypto-assets' is used to designate all the crypto-assets that are not regulated at EU level[12]. 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.

---

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

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

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

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

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

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

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

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

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

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

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

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

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

More information:

- on this consultation
- on the consultation document
- on the protection of personal data regime for this consultation

About you

* Language of my contribution

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

- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

- 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

Hubert

* Surname

d Etigny

* Email (this won't be published)

hubert.detigny@bnpparibas.com

* 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

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

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

* Organisation name

255 character(s) maximum

BNP Paribas

* 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.

78787381113-69

* Field of activity or sector (if applicable):

at least 1 choice(s)

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

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

- ○ Benchmark administrator
- ○ Benchmark contributor
- ○ Benchmark user
- ◉ Other

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

-

* Publication privacy settings

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

- ○ **Anonymous**
  Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.
- ◉ **Public**
  Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

☑ I agree with the personal data protection provisions

I. Questions for the general public

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

Question 1. Have you ever held crypto-assets?

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

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

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

II. Classification of crypto-assets

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

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

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

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

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

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

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

5.1 Please explain your reasoning for your answers to question 5:

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

We do believe that consideration should be given specifically to crypto-assets, i.e. digital assets "that may depend on cryptography and exists on a distributed ledger", as defined by the European Commission.

Indeed, it is the use of these technologies - cryptography and DLT-, which are common to the various assets at stake - “payment, investment, security, utility, hybrid tokens…” -, that differentiates them from other digital assets and thus creates specific issues, regarding for instance EU financial regulation, the fight against money laundering, financial stability, monetary policy or even sovereignty.

Broadening the focus to all digital assets would lead to considering assets that are too disparate in nature. It would raise issues too heterogeneous, potentially preventing operational conclusions from being reached.

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 deem it necessary to develop a European classification of the various types of crypto-assets. Such a classification would make it possible to define rules adapted to each of the different categories of assets thus defined.

Developing this classification at European level would (i) provide legal certainty for European actors, (ii) avoid regulatory arbitrations within Europe, (iii) contribute to the attractiveness of the EU.

Moreover, as a pioneer in the regulation of crypto-assets, the EU will strengthen its capacity to influence work on international standards in this area.

As crypto-assets are by nature rather flexible, adaptive, blurring traditional lines between different asset types (e.g. hybrid tokens), we believe this classification should remain agile to take into account the various characteristics and functionalities they may have.

A relevant approach, in line with the Lamfalussy process, should be to define broad categories of crypto-assets at the first level, i.e. the legislative one, while guidance, technical aspects and potential sub-categories should be addressed at the second level, by the ESAs (namely EBA and ESMA).

This flexible approach should make it possible to adapt, as swiftly as possible, the framework to future technological innovations.

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.

The classification, which should be set at the European level, could be based primarily on the crypto-asset's economic function, as proposed in this document.

Additional requirements related to the underlying assets (e.g. currencies, commodities, real estate, securities), the nature of the issuer (public authority, private entity), the legal rights attached, or the nature of the users (consumer, professional...) could also be considered when relevant.

In any case, the taxonomy should follow the "same business, same risks, same rules" principle, i.e. if the economic function and purpose of a crypto-asset are the same as a regulated asset class, it should be subject to the same set of financial and prudential rules. Any entity or intermediary engaging in crypto-assets activities that are equivalent to those performed by regulated financial entities or intermediaries, should be subject to the same legal requirements (in particular with respect to prudential and anti-money laundering

issues).

In France, at present, two types of crypto-assets are subject to specific regulations :

- utility tokens : the PACTE Bill, adopted in 2019, has established a framework for fundraising via initial coin offerings. The regime covers digital assets not classified as financial instruments, giving rise to one or more rights and that may be issued, registered, stored or transferred using a DLT ;

- unlisted security tokens : the ordinance of 8 December 2017 “on the use of shared electronic recording devices for the representation and transmission of financial securities”) allows the representation and transmission, using a DLT, of all financial securities, such as shares, bonds, collective investment undertakings…, that are neither eligible for the transactions of a central depositary nor delivered within a system for the settlement and delivery of financial instruments (i.e. unlisted).

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.

As regards “regulated” tokens, a distinction could be made between “quoted” and “unquoted” security tokens, as is already the case in France (see answer to previous question).

With respect to “unregulated” tokens, a distinction should be made between wholesale payment tokens and retail payment tokens. Indeed, given the users concerned by these different tokens - the financial institutions in the first case and the consumers in the second - the rules applicable may differ, for example in terms of protection of the user or with regard to rules on combating money-laundering and the financing of terrorism, which could imply for instance limits in terms of amount for retail payment tokens.

8.2 Please explain your reasoning for your answers to question 8:

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

The distinction between ‘payment tokens’, ‘investment tokens’, ‘utility tokens’ and ‘hybrid tokens’ is currently the most widespread and corresponds to the state of the art. These different categories seem broad enough to cover all current cases of use and could be used to define the main legislative principles at level 1.

However, in accordance with the Lamfalussy procedure and in order to have a regulatory framework that can be rapidly adapted to future developments, technical aspects and potential sub-categories of crypto-assets should be addressed by the ESAs at the second level.

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

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

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

As things stand, crypto-assets do not meet the criteria of the DGSD legal definition. According to the DGSD, a deposit "means a credit balance which results from funds left in an account or from temporary situations deriving from normal banking transactions and which a credit institution is required to repay under the legal and contractual conditions applicable, including a fixed-term deposit and a savings deposit".

It should be noted also that directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money states in :

- its recital 13 that "the issuance of electronic money does not constitute a deposit-taking activity […] ;
- its recital 18 that "electronic money needs to be redeemable […]. Redeemability does not imply that the funds received in exchange for electronic money should be regarded as deposits or other repayable funds […].

Furthermore Article 6 (3) confirms the above by stating that "any funds received by electronic money institutions from the electronic money holder shall be exchanged for electronic money without delay. Such funds shall not constitute either a deposit or other repayable funds received from the public […].

The statute of issuer of money-equivalent should not in any extent whatsoever be assimilated to an authorization to receive cash deposits or other repayable funds, such activity being highly regulated under EU law.

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

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

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

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

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

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

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

Improved liquidity and tradability of tokenised 'assets'	○	○	○	○	◉	○
Enhanced operational resilience (including cyber resilience)	○	○	○	◉	○	○
Security and management of personal data	○	○	○	◉	○	○
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.

Some of the crypto-assets could facilitate cross-border transactions.

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.

Benefits arising from market opportunities and user experience are more important than only technical benefits.

These benefits are conceivable and may be legitimately expected.
However, it is important to note that so far, they have not been proven, in the absence of sufficient experience.

On the contrary, some examples show different situations.

For instance, while the fact that crypto-assets transactions could be cheap is often put forward, there are concrete examples where the transaction fees generated are far too high for simple retail transactions. For example, the redemption fee on Tether can be up to 3%(*).

As regards ICOs, the comparison with IPOs, in terms of costs or efficiency, does not seem relevant to us. Indeed, IPOs and ICOs are designed to meet different needs, for example in terms of amounts raised, for different issuers, e.g. large companies vs fintech. IPOs also allow funds to be raised without dilution of capital.

As regards financial inclusion, the positive effect would be limited in Europe given the level already achieved in this area.

In any case, none of the potential benefits generally highlighted will be possible until all of the risks listed below are fully controlled. Effective responses to these risks are a prerequisite.

(*) source : “The role of crypto-assets in the payment system”, Banque de France, October 15 2019

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[16]. 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[17]. 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[18], this might change in the future.

[16] ESMA, “Advice on initial coin offerings and Crypto-Assets”, January 2019.

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

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

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

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

	1 (not important at all)	2	3	4	5 (very important)	Don’t know / no opinion / not relevant
Fraudulent activities	○	○	○	○	◉	○
Market integrity (e.g. price, volume manipulation, ...)	○	○	○	○	◉	○
Investor/consumer protection	○	○	○	○	◉	○
Anti-money laundering and CFT issues	○	○	○	○	◉	○
Data protection issues	○	○	○	○	◉	○
Competition issues	○	○	○	○	◉	○
Cyber security and operational risks	○	○	○	○	◉	○

Taxation issues	○	○	○	○	◉	○
Energy consumption entailed in crypto-asset activities	○	○	○	◉	○	○
Financial stability	○	○	○	○	◉	○
Monetary sovereignty/monetary policy transmission	○	○	○	○	◉	○

11.1 Is there any other important risks related to crypto-assets not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning:

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

In general, for all crypto-assets, the risks of legal uncertainty must also be taken into account, in addition to the risks mentioned here.

Other risks would be :
- a heterogeneous regulatory approach from one jurisdiction to another, leading to regulatory arbitrage and unlevel playing field ;
- non-compliance with international sanctions/embargoes programs ;
- related to the accounting of these assets.

On the question of energy consumption, while it is true that the technology currently dominant, i.e. the “proof of work” algorithm, used by the Bitcoin and Ethereum networks as system of consensus and validation of transactions, is very energy-intensive, it should be noted that other techniques, such as the "proof of stake" and the "proof of space", that require far less energy, are being developed. Actually, the crypto-assets ecosystem is the first to be affected by this issue of energy consumption and therefore the first to find innovative solutions to reduce it.

11.2 Please explain your reasoning for your answers to question 11:

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

Monetary sovereignty/monetary policy transmission and financial stability risks are perhaps the most significant, particularly in terms of potential consequences.

However, all the other risks identified - money laundering, cyber security, etc. - are also major and potentially linked to the issue of financial stability. None of them can be considered secondary.

That is why we consider that all these risks could have a major impact.
From a custodian point-of-view, the issue of investor and consumer protection is the most important.

The first priority of a custodian is to protect its investors and clients’ assets. As such, cyber security also represents an important risk.

“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.

The main expected benefits of stablecoins, compared to other crypto-assets, are their relative stability and trust (that may result from their stability). Concretely, the core value proposition of stablecoins is to provide a better store of value which allow to carry out transactions related to crypto-assets without leaving the DLT environment.

However, as emphasized by the G7 Working Group on Stablecoins, a global stable coin widely used as a store of value could potentially weaken the impact of monetary policy on domestic interest rates and credit conditions, particularly in countries whose currencies are not part of the reserve assets. Furthermore, none of the existing type of stablecoins - i.e. tokenised funds, off-chain collateralised stablecoins, on-chain collateralised stablecoins and algorithmic stablecoins - are as stable as a central bank or a commercial bank money (still 80% of the money created in the euro area) can be. Indeed, even in the case of tokenised funds, which are supposed to be the most efficient stablecoin in terms of stability, according to an ECB study(*), volatility risks still exist in the cases of fraud and operational accident.

In reality, only a CBDC (central bank digital currency) or a commercial bank digital currency, since they are different forms of a genuine money, can fully perform the functions of money : store of value, means of payment, unit of account. However, it seems that the impact the CBDC could have both in terms of financial stability (risk of “digital” bank run) and on the monetary policy transmission (cost and volume of bank lending and money creation) should be carefully monitored.

Moreover, as regards the financial markets, in order to carry out end-to-end transactions with “tokenised” assets on the blockchain, financial institutions need a liquid and safe asset for making settlements. A detailed analysis should be conducted to assess whether a CBDC and/or a European wholesale ledger for commercial bank digital currencies (that would be convertible at parity with the euro) would be the best solution to satisfy this need.

Commercial bank digital currencies could be an effective way to allow the circulation of money on a blockchain and make a perfectly safe and liquid payment instrument available on it without jeopardizing the current framework of monetary policy which has very much proved its worth. In any case, the development of an “e-euro” (whether CBDC and/or commercial bank digital currency) would significantly help blockchain-based financial services to scale up and would also enhance the attractiveness and international role of the

euro.

(*) “Stablecoins - no coins, but are they stable?”, EBC, In Focus, Issue n°3, November 2019

Question 13. In your opinion, what are the most important risks related to “stablecoins”?

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

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

13.1 Is there any other important risks related to “stablecoins” not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum

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

As with the other crypto-assets, legal uncertainty is a risk to be considered.

Also, as explained in the G7 Working Group on stablecoins report issued in October 2019 (“Investigating the impact of global stablecoins”), stablecoins, particularly payment tokens, may also have important implications for the funding of banks : “First, if users hold [global stablecoins] GSCs permanently in deposit-like accounts, retail deposits at banks may decline, increasing bank dependence on more costly and volatile sources of funding, including wholesale funding. In those countries whose currencies are part of the reserve, a portion of deposits drained from the banking system (when retail users buy GSCs) may revert to domestic bank deposits and short-term government securities. This implies that some banks may have larger wholesale deposits from stablecoin issuers rather than numerous small retail deposits”.

Stablecoins may also contribute to the occurrence of bank runs or even exacerbate such runs.

Finally, as a means of payment, stablecoins may have material negative impacts on safety, efficiency and integrity of payment systems, and thus on the financial stability. If they are not properly regulated, stablecoins may become the weak link jeopardising the payment system, whether at domestic or international level.
(see answer to question 12)

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.

We do not subscribe to this distinction between stablecoins and global stablecoins.

Indeed, we consider that any stablecoin arrangement has the potential to become global and most of the risks induced by stablecoins are not related to the size of these assets : legal certainty, money laundering, terrorist financing, stability of payment systems, cyber security, operational resilience, market integrity, data privacy, consumer protection, tax compliance. It is these different risks, taken individually or together, that create a potential threat to financial stability.

The distinction between wholesale and retail stablecoins, mentioned in question 26, seems more relevant for the design of appropriate regulations.

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

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

- Yes

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

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

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

Given their specificities, which derive from the technologies involved, given their potential benefits and given the material risks they induce, we do believe that a bespoke European regime for crypto-assets could be extremely positive for the European Union, particularly in terms of attractiveness, but also to preserve its financial sovereignty. Indeed, a sustainable ecosystem requires a “standard”, stability and trust. It also requires to deal with financial stability, competition and sovereignty issues. Only regulated approach can offer this.

The regime should be risk-based, proportional and should be agile enough to not hinder the ecosystem’s development. It should also follow the “same business, same risks, same rules” principle.

Moreover, we support an approach that does not result in distinct authorization and supervision regimes for crypto-assets qualifying as financial instruments and those which do not.

One of the main issues to be answered at EU level relates to the legal rights attached to crypto-assets. A clear definition of these rights and how they transfer would prevent further market fragmentation and regulatory arbitrage risks.

A bespoke regime could have the benefit or bringing more regulatory certainty on cross-border issues, define responsibilities, and even provide an arbitration mechanism if relevant.

However, as the development of such a regime might be long and complex, it would be interesting to consider, as a first step, the set up a European experimentation framework, which would allow the national competent authorities, under the European supervisory authorities (ESAs) supervision, to lift regulatory requirements to authorize specific projects. This experimental phase, properly framed, could contribute to the elaboration of the future European regime for crypto-assets.

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

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

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

As of today the French legal system provides for a special legal regime for “utility tokens”. Therefore, the French Market Authority (AMF) distinguishes two regimes, with on one hand that of financial securities which is applicable to the issuance of financial securities and would also apply to tokens that would have the same characteristics as financial securities with Security Token Offerings (STOs), and on the other hand that of ICOs which applies only to issuances of utility tokens.

The AMF offers the possibility of applying for an AMF visa for a public ICO. The Prospectus directive does not apply but the public ICO is subject to specific minimum constraints. In order to be able to request the optional visa of the AMF the issuer establishes an information document in accordance with article 712-2 of the general regulations of the AMF and the AMF instruction DOC- 2019-06. The token issuer must be constituted in the form of a legal person established or registered in France. The ICO contains in particular a process for monitoring and safeguarding the assets collected as part of the offer. The token issuer has set up a system enabling it to comply with its obligations in the fight against money laundering and the financing of terrorism, which are set out in articles L. 561-2 et seq. of the Monetary and Financial Code. The AMF also provides that information during the term of the offer must be clear, precise and exhaustive and that information must be provided annually to subscribers on the use of the assets collected.

The visa is an "optional label" which indicates that the AMF has verified that the Information Document is complete and understandable for investors. The project is supposed to gain visibility and possibly credibility by the 'label'.

These provisions do not make other ICOs illegal, but they cannot advertise publicly the offering of their tokens to potential investors.

For a start-up with an innovative project that uses blockchain, doing a Public ICO targeted by the AMF is therefore potentially an interesting way to approach new investors. On 17th December 2019 a first visa was established by the AMF for the ICO of French-ICO.

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

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

5000 character(s) maximum

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

All typologies of tokens should be included. A bespoke regime should 1) be focused on consumers protection and 2) not being restrictive on the tokens to be created (as long as the typologies of tokens are regulated with clear rules based on the underlying assets/values) – innovation will come in particular from the diversity. It should also – in our view - target the players allowed to operate the tokens – with specific license/registration rules etc. The idea here is to put generic (common to all tokens) risks like AML-TF etc. on the players and not to attach these risks to the tokens.

Question 17. Do you think that the use of crypto-assets in the EU would be facilitated by greater clarity as to the prudential treatment of financial institutions' exposures to crypto-assets (See the discussion paper of the Basel Committee on Banking Supervision (BCBS))?

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

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

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

Yes, with these instruments potentially becoming more sophisticated and widespread in the coming years, the EU and all stakeholders would benefit from more clarity regarding the prudential treatment of crypto-assets.

From a balance sheet standpoint for example, should an entity possess assets or liabilities relating to crypto-assets, it will have to know the conditions applying, i.e. regarding implications for the liquidity coverage ratio (LCR) and high-quality liquid assets (HQLA) eligibility.

More generally, from a prudential perspective, we see a strong need to develop the classification of the different types of crypto-assets, as suggested in this consultation paper. Indeed, without clear definitions of the various types of crypto-assets, treatment for high-risk crypto-assets, such as bitcoin, would be applied to crypto-assets that exhibit a lower-risk profile, such as stablecoins backed by fiat currency. A clear understanding and classification of different crypto-asset categories is needed to enable proper regulation and supervision according to their characteristics and risks.

In any case, any regulatory initiative regarding this prudential treatment of exposures to crypto-assets should ensure a level playing field between financial institutions and new entrants (including non-bank players coming from the tech area), following the "same business, same risks, same rules" principle.

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

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

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

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

Yes.
The tokenisation of assets involves the representation of pre-existing real assets issued through DLT or the issuance of tokens that are native through DLT. It will require the use of smart contracts.

To ensure the tokenisation of assets, it's important to provide legal certainty. At this stage, legal certainty is questionable on some points (ownership, governing law, identification of the parties…) and smart contracts are still relatively untested in courts. To reduce risk of regulatory arbitrage within EU and to ensure competitiveness of the EU, we should try to harmonize as much as possible national civil laws. However, it has to be noted that such a harmonization of civil laws is an ambitious objective.

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

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

Question 19. Can you indicate the various types and the number of service providers related to crypto-assets (issuances of crypto-assets, exchanges, trading platforms, wallet providers, ...) in your jurisdiction?

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

In France, the PACTE Bill, adopted in 2019, sets out a framework for the "digital assets services providers" (DASP) offering the following services :

1. services on behalf of third parties :

- custody of digital assets, meaning in practice the custody of cryptographic keys on behalf of a client ;
- the service of buying or selling digital assets for legal tender ;
- the service of trading digital assets for other digital assets ;
- the reception and transmission of orders for digital assets, meaning the act of receiving and transmitting buy or sell orders for digital assets on behalf of a client ;
- the management of digital asset portfolios, meaning the act of managing, on a discretionary, client-by-client basis, portfolios that include one or more digital assets under a mandate given by a client ;
- advice to investors in digital assets. This means giving personalized recommendations to a third party, either at their request or on the initiative of the service provider providing the advice, concerning one or more digital assets ;

- digital asset underwriting, meaning the act of purchasing digital assets directly from a digital asset issuer, with a view to subsequently selling them ;
- the guaranteed investment of digital assets, which consists in searching for buyers on behalf of a digital asset issuer and guaranteeing them a minimum amount of purchases by undertaking to buy any digital assets that are not placed ;
- the unsecured investment of digital assets, meaning the act of searching for buyers on behalf of a digital asset issuer without guaranteeing them an amount of purchases.

2. the operation of a trading platform for digital assets. This concerns the management of one or more digital asset trading platforms, within which multiple buying and selling interests expressed by third parties for digital assets in exchange for other digital assets or a currency that is legal tender can interact in such a way as to result in the conclusion of contracts.

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.

To secure potential litigation – notably from a consumer protection standpoint – a representative located in the EU and a proper approval/visa by the competent authority before the issue should be mandatory. An EU crypto-assets framework should not deprive EU consumers of their rights to EU litigation settlement principles.

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

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

Question 21.1 Please indicate the entity that, in your view, should be responsible for this disclosure (e.g. the issuer/sponsor, the entity placing the crypto-assets in the market) and the content of such information (e.g. information on the crypto-asset issuer, the project, the rights attached to the crypto-assets, on the secondary trading, the underlying technology, potential conflicts of interest, ...):

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

In the case of the ICO, it is the issuer that should be responsible for the publication of the information document, as in the case in France under the PACT Bill. According to the article 712-2 of the AMF General Regulation, for the ICO, "the information document shall contain all the information concerning the token issuer and the planned token offering needed to enable subscribers to make an informed investment decision and understand the risks relating to the offering.

This information shall include the following:

1. A detailed description of the token issuer's project, the token offering, the reasons for the offering and the planned use of the funds and digital assets collected via the offering ;
2. A detailed description of the rights and obligations attached to the tokens and the procedures and conditions of exercise of these rights ;
3. A detailed description of the characteristics of the offering, in particular the number of tokens to be issued, the token issue price, the subscription terms and conditions and the minimum amount necessary to carry out the project and the maximum amount of the offering ;
4. The technical specifications of the token issue ;
5. A detailed description of the means implemented to ensure monitoring and safeguarding of the funds and digital assets collected via the offering, as defined in Article 712-7 ;
6. A description of the key characteristics of the token issuer and a presentation of the main participants involved in the project's design and development ; and
7. The risks relating to the token issuer, the tokens, the token offering and the carrying out of the project.

All such information shall be fair, clear and not misleading and shall be presented in a concise and comprehensible form."

Question 22. If a requirement to provide the information on the offers of crypto-assets is imposed on their issuer/sponsor, would you see a need to

clarify the interaction with existing pieces of legislation that lay down information requirements (to the extent that those rules apply to the offers of certain crypto-assets, such as utility and/or payment tokens)?

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
The Consumer Rights Directive	○	○	○	○	◉	○
The E-Commerce Directive	○	○	◉	○	○	○
The EU Distance Marketing of Consumer Financial Services Directive	○	○	○	○	◉	○

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.

Other texts may need to be taken into consideration but further work is needed to identify them.

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.

We believe that "Investments tokens" and "hybrid tokens covering investments" should at least be concerned by these commitments in order to maintain proper information regarding transparency - notably on prices and execution – key characteristics and risks. Related legislation should therefore be identified and updated.

Question 23. Beyond any potential obligation as regards the mandatory incorporation and the disclosure of information on the offer, should the crypto-asset issuer or sponsor be subject to other requirements?

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

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

23.1 Is there any other requirement not mentioned above to which the crypto-asset issuer should be subject? Please specify which one(s) and explain your reasoning:

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

We believe that crypto-asset issuer should be subject to full anti money laundering (notably KYC) and counter terrorism financing requirements. Crypto-assets should not be used to ease creation and circulation of alternative assets values for criminal purposes. A particular attention should be paid to the circumvention of taxes and EU sanctions and embargoes regulation principles.

23.2 Please explain your reasoning for your answers to question 23:

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

The regulation framework should at least not be different than the regulation framework that would be applicable to the issuing of real investments assets.

1.2. Issuance of "stablecoins" backed by real assets

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

Question 24. In your opinion, what would be the objective criteria allowing for a distinction between "stablecoins" and "global stablecoins" (e.g. number and value of "stablecoins" in circulation, size of the reserve, ...)? Please explain your reasoning.

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

As stated in answer to question 13.2, we believe that any stablecoin arrangement has the potential to become global and thus should be regulated regardless of size.

Question 25.1 To tackle the specific risks created by "stablecoins" and "global stablecoins", what are the requirements that could be imposed on their issuers and/or the manager of the reserve?

Please indicate for "stablecoins" if each is proposal is relevant.

	Relevant		Don't know /

		Not relevant	no opinion
The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)	◉	○	○
The issuer should contain the creation of “stablecoins” so that it is always lower or equal to the value of the funds of the reserve	◉	○	○
The assets or funds of the reserve should be segregated from the issuer’s balance sheet	◉	○	○
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	◉	○	○
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	◉	○	○
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	◉	○	○
Obligation for the assets or funds to be held in custody with credit institutions in the EU	◉	○	○
Periodic independent auditing of the assets or funds held in the reserve	◉	○	○
The issuer should disclose information to the users on (i) how it intends to provide stability to the “stablecoins”, (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve	◉	○	○
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	◉	○	○
Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer	◉	○	○

Question 25.1 To tackle the specific risks created by “stablecoins” and “global stablecoins”, what are the requirements that could be imposed on their issuers and/or the manager of the reserve?

Please indicate for “stablecoins” if each is proposal is relevant.

	Relevant	Not relevant	Don’t know / no opinion

The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)	◉	○	○
The issuer should contain the creation of “stablecoins” so that it is always lower or equal to the value of the funds of the reserve	◉	○	○
The assets or funds of the reserve should be segregated from the issuer’s balance sheet	◉	○	○
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	◉	○	○
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	◉	○	○
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	◉	○	○
Obligation for the assets or funds to be held in custody with credit institutions in the EU	◉	○	○
Obligation for the assets or funds to be held for safekeeping at the central bank	◉	○	○
Periodic independent auditing of the assets or funds held in the reserve	◉	○	○
The issuer should disclose information to the users on (i) how it intends to provide stability to the “stablecoins”, (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve	◉	○	○
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	◉	○	○
Obligation for the issuer to use open source standards to promote competition	◉	○	○

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

5000 character(s) maximum

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

We believe that stablecoins issuers should be subject to full anti money laundering (notably KYC) and counter terrorism financing requirements. Stablecoins should not be used to ease creation and circulation of alternative assets values for criminal purposes. A particular attention should be paid to the circumvention of taxes and EU sanctions and embargoes regulation principles.
Same requirements should be applicable to the manager of the reserve.

25.1 b) Please Please illustrate your responses to question 25.1:

5000 character(s) maximum

It is of the utmost importance to avoid, fraud, money laundering, terrorist financing, tax evasion by stablecoin issuers and manager of the reserve.

In addition, the use of safe and liquid assets, the strict reflect of the stablecoin value by the reserve, the absence of encumbrance, the disclosing of information and the open source standards will protect consumers' interests.

Segregation of funds, prudential requirements, insolvency rules, custodian rules, audit and disclosure principles will permit to ease stablecoins use as a "safe alternative" for transactions.

Question 25.2 To tackle the specific risks created by "stablecoins" and "global stablecoins", what are the requirements that could be imposed on their issuers and/or the manager of the reserve?

Please indicate for "global stablecoins" if each is proposal is relevant.

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

The issuer should disclose information to the users on (i) how it intends to provide stability to the "stablecoins", (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve	◉	○	○
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	◉	○	○

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

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

We believe that global stablecoins issuers should be subject to full anti money laundering (notably KYC) and counter terrorism financing requirements. Global stablecoins should not be used to ease creation and circulation of alternative assets values for criminal purposes. A particular attention should be paid to the circumvention of taxes and EU sanctions and embargoes regulation principles.
Same requirements should be applicable to the manager of the reserve.

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

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

It is of the utmost importance to avoid, fraud, money laundering, terrorist financing, tax evasion by global stablecoin issuers and manager of the reserve.

In addition, the use of safe and liquid assets, the strict reflect of the global stablecoin value by the reserve, the absence of encumbrance, the disclosing of information and the open source standards will protect consumers' interests.

Segregation of funds, prudential requirements, insolvency rules, custodian rules, audit and disclosure principles will permit to ease global stablecoins use as a "safe alternative" for transactions.

"Stablecoins" could be used by anyone (retail or general purpose) or only by a limited set of actors, i.e. financial institutions or selected clients of financial institutions (wholesale). The scope of uptake may give rise to different risks. The G7 report on "investigating the impact of global stablecoins" stresses that "*Retail stablecoins, given their public nature, likely use for high-volume, small-value payments and potentially high adoption rate, may give rise to different risks than wholesale stablecoins available to a restricted group of users*".

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

- ◉ Yes
- ○ No

Don’t know / no opinion / not relevant

26.1 Please explain your reasoning for your answer to question 26:

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

Wholesale stablecoins are used to facilitate transactions between financial institutions, while retail stablecoins are designed for consumers. This second category, given the users concerned, i.e. retail customers, implies specific rules, for example in terms of consumer protection or with regard to rules on combating money-laundering and the financing of terrorism, which could imply for instance limits in terms of amount for retail payment tokens.

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[19] while others use simple and inexpensive technology.

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

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

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don’t know / no opinion / not relevant
Absence of accountable entity in the EU	○	○	○	○	◉	○
Lack of adequate governance arrangements, including operational resilience and ICT security	○	○	○	○	◉	○

Absence or inadequate segregation of assets held on the behalf of clients (e.g. for 'centralised platforms')	○	○	○	○	◉	○
Conflicts of interest arising from other activities	○	○	○	○	◉	○
Absence/inadequate recordkeeping of transactions	○	○	○	○	◉	○
Absence/inadequate complaints or redress procedures are in place	○	○	○	○	◉	○
Bankruptcy of the trading platform	○	○	○	○	◉	○
Lacks of resources to effectively conduct its activities	○	○	○	○	◉	○
Losses of users' crypto-assets through theft or hacking (cyber risks)	○	○	○	○	◉	○
Lack of procedures to ensure fair and orderly trading	○	○	○	○	◉	○
Access to the trading platform is not provided in an undiscriminating way	○	○	◉	○	○	○
Delays in the processing of transactions	○	○	○	○	◉	○
For centralised platforms: Transaction settlement happens in the book of the platform and not necessarily recorded on DLT. In those cases, confirmation that the transfer of ownership is complete lies with the platform only (counterparty risk for investors vis-à-vis the platform)	○	○	○	○	◉	○
Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse	○	○	○	○	◉	○

27.1 Is there any other main risks posed by trading platforms of crypto-assets not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum

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

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.

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 28. What are the requirements that could be imposed on trading platforms in order to mitigate those risks?

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

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

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

28.1 Is there any other requirement that could be imposed on trading platforms in order to mitigate those risks? Please specify which one(s) and explain your reasoning:

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

We do not see other requirement that could be imposed on trading platforms in order to mitigate those risks.

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.

Investments tokens, stablecoins and hybrid tokens (based on investments tokens or stablecoin) should at least be considered for these requirements. All requirements are highly relevant to protect users, funds and assets. They should remain the same than for the trading platforms of real assets.

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

Crypto-asset exchanges are entities that offer exchange services to crypto-asset users, usually against payment of a certain fee (i.e. a commission). By providing broker/dealer services, they allow users to sell their crypto-assets for fiat currency or buy new crypto-assets with fiat currency. It is important to note that some exchanges are pure crypto-to-crypto exchanges, which means that they only accept payments in other crypto-assets (for instance, Bitcoin). It should

also be noted that many cryptocurrency exchanges (i.e. both fiat-to-crypto and crypto-to-crypto exchanges) operate as custodial wallet providers (see section III.B.4 below). Many exchanges usually function both as a trading platform and as a form of exchange (study from the European Parliament on “Cryptocurrencies and Blockchain”, July 2018).

Question 29. In your opinion, what are the main risks in relation to crypto-to-crypto and fiat–to-crypto exchanges?

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

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

29.1 Is there any other main risks in relation to crypto-to-crypto and fiat–to-crypto exchanges not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning:

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

We believe that crypto-to-crypto and fiat-to-crypto exchanges should be subject to full anti money laundering (notably KYC) and counter terrorism financing requirements. crypto-to-crypto and fiat-to-crypto exchanges should not be used to ease creation and circulation of alternative assets values for criminal purposes. A particular attention should be paid to the circumvention of taxes and EU sanctions and embargoes regulation principles.

29.2 Please explain your reasoning for your answer to question 29:

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

Question 30. What are the requirements that could be imposed on exchanges in order to mitigate those risks?

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

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

Exchanges should have an adequate complaints handling and redress procedures	○	○	○	○	◉	○
Exchanges should be subject to prudential requirements (including capital requirements)	○	○	○	○	◉	○
Exchanges should be subject to advertising rules to avoid misleading marketing/promotions	○	○	○	○	◉	○
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)	○	○	○	○	◉	○
Exchanges should be responsible for screening crypto-assets against the risk of fraud	○	○	○	○	◉	○

30.1 Is there any other requirement that could be imposed exchanges in order to mitigate those risks? Please specify which one(s) and explain your reasoning:

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

We do not see other requirement to mitigate those risks.

30.2 Please indicate if those requirements should be different depending on the type of crypto-assets available on the exchange and explain your reasoning for your answers to question 30:

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

We do not see differences depending of the type of crypto-assets available. All the items are highly relevant to ensure consumers protection, restrict criminality and to limit market abuses.

4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys[20] 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[21]. DLT networks generally provide their own wallet functions (e.g. Bitcoin or Ether).

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

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

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

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

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
No physical presence in the EU	○	○	○	○	◉	○
Lack of adequate governance arrangements, including operational resilience and ICT security	○	○	○	○	◉	○
Absence or inadequate segregation of assets held on the behalf of clients	○	○	○	○	◉	○
Conflicts of interest arising from other activities (trading, exchange)	○	○	○	○	◉	○
Absence/inadequate recordkeeping of holdings and transactions made on behalf of users	○	○	○	◉	○	○
Absence/inadequate complaints or redress procedures are in place	○	○	◉	○	○	○
Bankruptcy of the custodial wallet provider	○	○	○	○	◉	○
Inadequate own funds to repay the consumers	○	○	○	○	◉	○

Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)	○	○	○	○	◉	○
The custodial wallet is compromised or fails to provide expected functionality	○	○	○	○	◉	○
The custodial wallet provider behaves negligently or fraudulently	○	○	◉	○	○	○
No contractual binding terms and provisions with the user who holds the wallet	○	○	○	◉	○	○

31.1 Is there any other risk in relation to the custodial wallet service provision not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning:

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

Another risk lies in the potential difficulty of modifying past transaction records that have been validated and appended on a DLT. The risk of not being able to reverse a crypto-asset transfer should not be overlooked.

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.

While crypto-assets may bring new types of risks not fully covered by existing regulations, we believe they also carry traditional risks. As such, we are in favor of an approach that provides the same level of investor protection and guarantees for investors.

Question 32. What are the requirements that could be imposed on custodial wallet providers in order to mitigate those risks?

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

						Don't know /

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

32.1 Is there any other requirement that could be imposed on custodial wallet providers in order to mitigate those risks? Please specify which one(s) and explain your reasoning:

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

We believe that custodial wallet providers should be subject to full anti money laundering (notably KYC) and counter terrorism financing requirements. Custodial wallet providers should not be used to ease circulation of alternative assets values for criminal purposes. A particular attention should be paid to the circumvention of taxes and EU sanctions and embargoes regulation principles.
The establishment of a comprehensive DLT security approach addressing all aspects of the DLT key

management lifecycle would also bring more guarantees to investors. DLT-specific security considerations regarding the creation, maintenance, storage and disposal of sensitive key information would be beneficial.

32.2 Please indicate if those requirements should be different depending on the type of crypto-assets kept in custody by the custodial wallet provider and explain your reasoning for your answer to question 32:

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

We do not see differences based on the typology of crypto-assets. All proposed items are highly relevant to protect users, funds and assets. They should remain the same than for the custody of real assets.

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

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

33.1 Please explain your reasoning for your answer to question 33:

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

Custodial wallet providers will play an important role in a context of strong risks arising from the loss of private keys - from a consumer protection standpoint. Moreover, custodial wallet providers could play an important role to prevent money laundering and terrorism financing.

We share the OECD's analysis(*) that despite its potential for disintermediation at many levels, tokenisation of assets will ultimately depend on the existence of a trusted and credible central authority that will guarantee the connection of the off-chain world to the distributed ledger environment.

As such, this implies a central role for custodians, gaining a key role in the structure of tokenised markets as the centralised trusted authority ensuring the smooth connection of the on-chain platform to the off-ledger environment.

For instance, they may be called to act as the trusted party that will guarantee the backing of tokens issued by the real assets, as well as hold such assets in custody.

Custodians will also need to ensure that the digital representation of the asset on the ledger is unique and that the same asset is not being represented by multiple tokens in multiple platforms..

This role is not limited to onboarding and transitioning from the off-chain to the on-chain world, but importantly, involves the safeguarding or the asset. Adequate safekeeping of assets backing tokens at all times will need to be ensured, similar to conventional custodianship

(*) OECD (2020), The Tokenisation of assets and Potential Implications for Financial Markets, www.oecd.org /finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-FinancialMarkets.html)

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

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

The operation of crypto-assets payments on behalf of should be in the regulated space (same principle than for the EU 2015/2366 Directive). Advisory activities should also be regulated on the same basis than “real assets”.

Another issue that should be examined is the definition of the service of custody of crypto-assets for a third-party. In France, the service of custody of digital assets’ defining criterion is the control of the means of access to the crypto-assets. However, some business models are structured with a purely technical provider offering custody solutions (e.g. through multi-party computation (MPC).

We believe the EU definition of the service of custody of crypto-assets should thus reflect the diversity of custody set-ups in this area, and exclude purely technical providers of custody solutions from the definition of the service of custody of crypto-assets itself.

5. Other services providers

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

Question 35. In your view, what are the services related to crypto-assets that should be subject to requirements?

(When referring to execution of orders on behalf of clients, portfolio management, investment advice, underwriting on a firm commitment basis, placing on a firm commitment basis, placing without firm commitment basis, we consider services that are similar to those regulated by Annex I A of MiFID II.)

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

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

35.1 Is there any other services related to crypto-assets not mentioned above that should be subject to requirements? Please specify which one(s) and explain your reasoning:

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

We do not see other services related to crypto-assets that should be subject to requirements.

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.

We identified, on a risk based approach, that:

- items classified “5” should be subject to license due to AML-TF strong risks in relation with the “direct” provision of services involving the receipt of funds or crypto-assets ;
- items classified “2” should be subject to license only if provided with other licensed activities ;
- items classified “4” should be subject to less restrictive license, similar to asset management regulation.

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.

Transactions involving crypto-assets should be subject to full anti money laundering (notably KYC) and counter terrorism financing requirements (same basis than PSD2).

Moreover, strong authentication and “execution” rules are keys to frame these services and prevent fraud.

C. Horizontal questions

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

1. Market Integrity

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

Question 37. In your opinion, what are the biggest market integrity risks related to the trading of crypto-assets?

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

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

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.

Yes, the lack of transparency of operators and of the products, and more specifically the owner of the crypto-asset wallet.

The use of High Frequency Trading of crypto-assets could also imply increased market integrity risks.

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.

Crypto-assets are complex, volatile, not always liquid and often-leveraged products based on exchange tokens with underlying market integrity issues.

Liquidity is typically shallow and investors may have a limited possibility of liquidating an investment.

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.

Making digital assets safer, more transparent and more credible requires specialized surveillance, monitoring and compliance tools designed uniquely for crypto markets. It also requires specialized rules.

Others solution could be envisaged, as developing a practical Code of Conduct for Market Integrity and providing an agreement / Membership to the operators to select and check them and to give them responsibility on the market. And also having strong governance rules on crypto trading platforms.

While the information on executed transactions and/or current balance of wallets are often openly accessible in distributed ledger based crypto-assets, there is currently no binding requirement at EU level that would allow EU

supervisors to directly identify the transacting counterparties (i.e. the identity of the legal or natural person(s) who engaged in the transaction).

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

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

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

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

Digital identify and/or KYC registry attached to the public keys combined with strong authentication mechanisms for the transactions could be used.

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.

Supervisors should be able to formally identify the parties for the transactions in crypto-assets in order to enforce market abuses regulation principles and to deal with litigations. Obtaining parties identity is crucial for any investigations and for market security.

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 suggest, once a client is registered in the EU with a service provider, the Implementation of a double validation mechanism (client level + service provider level) prior to crypto-assets transactions.

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.

A bespoke regulation should fully encompass AML/CFT principles arising from FATF recommendations. Aligned Definitions are keys to the creation of a proper and accurate monitoring framework. The development of automated monitoring tools and rules will rely on the definition alignment.

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

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

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

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

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

The following players should be added to the EU AML/CFT legal framework obligations on a risk based approach: "Custodian", "funds", "distributors", "token vs token operators". It is important to underline that these players will directly deal either with crypto-assets or with underlying financial flows. They will therefore face the same needs to identify parties, origin of funds and to clarify transactions purposes.

We do believe that any "collection on behalf of", or "payment on behalf of" activity in relation with crypto-assets should be subject to AML/CFT requirements (same principles than PSD2).

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

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

We would like to highlight that all these activities can actively play an important role in the AML-CTF prevention. Besides, the bespoke regime should reflect the fiat money regime commitments to avoid circumvention of the AML-CTF principles.

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.

All these activities can actively play an important role in the AML-CTF prevention. Besides, the bespoke regime should reflect the fiat money regime commitments to avoid circumvention of the AML/CFT principles.

However, not all EU jurisdictions have defined what a crypto-asset service provider is. As such, a prerequisite would be to have an EU definition of what constitutes a crypto-asset service provider, to effectively guarantee they are subject to the EU AML/CFT framework.
In this perspective, the principles defined in the French “PACTE” law in 2019 regarding the Digital Asset Service Provider (DASP) could be represented.

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.

The AML/CFT risks arising from peer-to-peer transactions could be mitigated by the implementation of “digital identity” mechanisms. A dedicated smart contract could be created in order to confirm the “digital identity” control validity. A tax purposes registration commitment could also be studied.

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

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

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

45.1 Please explain your reasoning for your answer to question 45:

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

It could be technically too complicated to implement these requirements without a proper implementation methodology.

Question 46. In your view, do you consider relevant that the following requirements are imposed as conditions for the registration and licensing of providers of services related to crypto-assets included in section III. B?

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Directors and senior management of such providers should be subject to fit and proper test from a money laundering point of view, meaning that they should not have any convictions or suspicions on money laundering and related offences	○	○	○	○	◉	○
Service providers must be able to demonstrate their ability to have all the controls in place in order to be able to comply with their obligations under the anti-money laundering framework	○	○	○	○	◉	○

46.1 Please explain your reasoning for your answer to question 46:

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

We do believe that crypto-assets providers of services should at least be subject to the same licenses principles than “fiat money” providers of services. The use of crypto-assets should not permit to circumvent “fiat money” regulation principles.

3. Consumer/investor protection[21]

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[22]. Offerings of utility tokens, for instance, do not provide for minimum investment amounts nor are they necessarily limited to professional or sophisticated investors. When considering the consumer protection, the functions of the crypto-assets should also be taken into consideration. While some crypto-assets are bought for investment purposes, other are used as a means of payment or for accessing a specific product or service. Beyond the information that is usually provided by crypto-asset issuer or sponsors in their 'white papers', the question arises whether providers of services related to crypto-assets should carry out suitability checks depending on the riskiness of a crypto-asset (e.g. volatility, conversion risks, ...) relative to a consumer's risk appetite. Other approaches to protect consumers and investors could also include, among others, limits on maximum investable amounts by EU consumers or warnings on the risks posed by crypto-assets.

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

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

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

Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Information provided by the issuer of crypto-assets (the so-called 'white papers')	○	○	○	○	◉	○
Limits on the investable amounts in crypto-assets by EU consumers	○	○	○	○	◉	○
Suitability checks by the crypto-asset service providers (including exchanges, wallet providers, ...)	○	○	○	○	◉	○
Warnings on the risks by the crypto-asset service providers (including exchanges, platforms, custodial wallet providers, ...)	○	○	○	○	◉	○

47.1 Is there any other type of consumer protection measures that could be taken as regards crypto-assets? Please specify which one(s) and explain your reasoning:

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

Information provided by the distributor of crypto-assets (on the basis of the information provided by the issuers) to be tailored to a profile of investor in order to be sufficiently clear and not misleading and allowing for an allowed decision.

Suitability checks by the crypto assets provider in order to make sure that the crypto assets meet the client situation and need.

Product governance rules to ensure that only products with a potential interest for clients are created /proposed.

Conflicts of interests rules should also apply to crypto assets.

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.

General principles of clients protection (i.e.: information, suitability and primacy of client interests) should apply to all types of crypto assets as they already apply to all types of banking and investment products. Additional measures like enhanced information should be implemented for investments tokens and hybrid tokens.

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.

Customer protection general principles should be implemented depending on specific circumstances (types of crypto assets, customer profile, distribution channels and sales practices…) according to the

proportionality principle. “Standard” Investor protection arising from MiFID should at least be implemented for the investments tokens.

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.

Customer protection general principles should be implemented depending on specific circumstances (types of crypto assets, customer profile, distribution channels and sales practices…) according to the proportionality principle.

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

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

50.1 Please explain your reasoning for your answer to question 50:

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

Customer protection general principles should be implemented depending on specific circumstances (types of crypto assets, customer profile, distribution channels and sales practices…) according to the

proportionality principle. However, it is important to underline that as long as tokens represent a value or an asset, there is a risk (AML-TF, loss, fraud/abuses) for the consumer/investor.

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

Question 51. In your opinion, how should the crypto-assets issued in third countries and that would not comply with EU requirements be treated?

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

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

51.1 Is there any other way the crypto-assets issued in third countries and that would not comply with EU requirements should be treated? Please specify which one(s) and explain your reasoning:

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

Crypto-assets issued in third countries and that do not comply with EU requirements should be banned, from a consumer and investor protection perspective.

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.

It will not be possible to ensure EU consumers protection (especially from a market abuse standpoint) and to prevent AML-TF risks.

4. Supervision and oversight of crypto-assets service providers

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

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

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

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

All crypto-asset service providers should be subject to supervisory coordination and/or supervision by EU authorities, notably in order to enforce AML-TF and investment regulations.

A possible approach could be to adapt supervision depending on the type of activity/risks that are at play for each crypto-asset service provider.

Exemption thresholds based on quantitative criteria could ensure an appropriate supervision mechanism for riskier providers. Proportionality is key so as not to stifle innovation.

Another advantage of supervisory coordination or supervision by EU authorities would be that it could monitor more efficiently risks at EU level.

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.

We suggest at least an investigation tool allowing to "follow" traceability of the crypto assets on the blockchain. A public key registry access could also be important.

We are of the view that the establishment of a supervisory college at EU level would be beneficial for effective supervision. This college should logically be part of the supervisory body of the European Central Bank.

One could also imagine a supervisory entity acting as a node on relevant DLT networks for instant monitoring.

Other useful tools would be a discipline regime with sanctions for non-compliant players and investigative powers when circumstances require it.

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[23] 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.

---

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

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

Current trends concerning security tokens

For the purpose of the consultation, we consider the instances where security tokens would be admitted to trading or traded on a trading venue within the meaning of MiFID. So far, however, there is evidence of only a few instances of security tokens 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.

From a security token perspective, France has adopted in 2017 a blockchain ordinance which has the goal to give a legal framework for the trading of unlisted securities using DLT.

There have also been tests recently conducted in the UK for STO issuances on Turquoise MTF : the London Stock Exchange (LSE) has worked with the Fintech Company 20|30 to issue their first tokenized securities under the Financial Conduct Authority (FCA) Sandbox 4 program. The £3 million worth of security tokens were issued and settled through LSE's MTF Turquoise equity trading service.

Question 55. Do you think that DLT could be used to introduce efficiencies or other benefits in the trading, post-trade or asset management areas?

- (●) Completely agree
- ( ) Rather agree
- ( ) Neutral
- ( ) Rather disagree
- ( ) Completely disagree
- ( ) Don't know / no opinion / not relevant

If you agree with question 55, please indicate the specific areas where, in your opinion, the technology could afford most efficiencies when compared to the legacy system:

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

55.1 Please explain your reasoning for your answer to question 55:

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

DLT has significant cost saving implications for companies spending large amounts of money to maintain, update, and secure a centralized service. It provides a guarantee of recording and has innate structural security benefits.

Centralized networks create a single point of failure for all connected services, while devices on a distributed network are more autonomous and not reliant on a core system. Any malicious attempts to alter or attack a distributed database would require penetration of a majority of connected nodes, out of potentially thousands, making it virtually impossible to hack. Utilizing a distributed architecture with DLT that enables devices to communicate directly with each other will enhance the capabilities of device management. By connecting peer-to-peer (P2P), rather than through a central broker, actions can be disseminated in a highly controlled, streamlined fashion.

Audit trail : one of the main benefits of DLT is the immutability of its ledger and the ability, therefore, to audit all events in the ledger. Changes to the ledger that have been successfully authenticated cannot be deleted or modified: this ensures the accuracy and security of the record. Data Reliability As changes to a distributed database are required to undergo multiple levels of DLT validation, the risk of inaccurate or junk data being consumed for analytics is greatly reduced.

DLT could be a gain of time in the settlement process, and the self-execution of contractual parts such as selling restrictions would increase efficiency of rules execution, which could be used throughout trading and post-trading, and in asset management.

Settlement via DTL would allow getting an immediate picture of the company shareholders, contributing especially to an increasing transparency of the post trading phase and also before the trading as all parties will have access to the same documents.
Tokens could be a unique kind of diversified asset class.

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.

As of today, the volume of tests conducted does not allow us to provide for an opinion on an eventual increase of financial stability risk with the use of DLT for the trading and post trading of financial instruments. More tests should be conducted in order to position ourselves. An European regulatory sandbox is needed to increase the number of initiatives regarding the trading and post trading through DLT and to allow stakeholders to assess the risk.

Question 57. Do you consider that DLT will significantly impact the role and operation of trading venues and post-trade financial market infrastructures (CCPs, CSDs) in the future (5/10 years’ time)? Please explain your reasoning.

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

We believe that DLT could impact deeply the role and operation of trading venues and post trade financial market infrastructures in the future, since it is peer-to-peer and avoids intermediaries. Especially in the fields of clearing, depository, settlement, and trusted third party roles.

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.

The market does not exist yet and therefore has to be created.
The aim is to create a European experimentation framework, which would allow national competent authorities, under the ESAs’ supervision, to establish regulatory sandboxes within which they could deploy new DLT solutions in a fast and scalable manner. This sandbox environment would allow the parties to learn and work constructively together. A gradual regulatory approach could then be elaborated step by step as regulators and market initiatives mature. The framework should be elaborated by the EU Commission.

B. Assessment of legislation applying to ‘security tokens’

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

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

1.1 Financial instruments

Under MiFID, financial instruments are specified in Section C of Annex I. These are inter alia ‘transferable securities’, ‘money market instruments’, ‘units in collective investment undertakings’ and various derivative instruments. Under Article 4(1)(15), ‘transferable securities’ notably means those classes of securities which are negotiable on the capital market, with the exception of instruments of payment.

There is currently no legal definition of security tokens in the EU financial services legislation. Indeed, in line with a functional and technologically neutral approach to different categories of financial instruments in MiFID, where security tokens meet necessary conditions to qualify as a specific type of financial instruments, they should be regulated as such. However, the actual classification of a security token as a financial instrument is undertaken by National Competent Authorities (NCAs) on a case-by-case basis.

In its Advice, ESMA indicated that in transposing MiFID into their national laws, the Member States have defined specific categories of financial instruments differently (i.e. some employ a restrictive list to define transferable securities,

others use broader interpretations). As a result, while assessing the legal classification of a security token on a case by case basis, Member States might reach diverging conclusions. This might create further challenges to adopting a common regulatory and supervisory approach to security tokens in the EU.

Furthermore, some 'hybrid' crypto-assets can have 'investment-type' features combined with 'payment-type' or 'utility-type' characteristics. In such cases, the question is whether the qualification of 'financial instruments' must prevail or a different notion should be considered.

Question 59. Do you think that the absence of a common approach on when a security token constitutes a financial instrument is an impediment to the effective development of security tokens?

- (●) Completely agree
- ( ) Rather agree
- ( ) Neutral
- ( ) Rather disagree
- ( ) Completely disagree
- ( ) Don't know / no opinion / not relevant

59.1 Please explain your reasoning for your answer to question 59:

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

The existence of several NCA definitions of what is a token that should qualify as a financial instrument creates difficulties in developing a security tokens European market, and, as noted in ESMA note, creates regulation and supervision.

Lack of convergence towards a common approach has been problematic for market participants who operate in multiple jurisdictions, defining a common regulatory perimeter could improve innovation and reduce as well compliance costs linked to implementation of multiple sets or rules and overall costs.

Having a common approach on the perimeter of what constitutes a security token and how to improve transparency, disclosure and investor protection would help in the creation of a larger investor base and a secure cross-country tokens market.

The absence of a clear definition of what is a security token at the European level is an impediment to the development of the security tokens market since tokens are by essence issued for an investor base rather selected upon its appetence for the particular token issued than on its appurtenance to a specific State.

Discrepancies on the understanding and definition of a security token as a financial instrument could lead to distortion within the European market, eventually to taxation issues or the ban within some jurisdictions. On the contrary, a common approach would bring more regulatory certainty, facilitate the exchanges of token in trading venues, ease the issuance process with an international investor base and prevent tax issues (or accountability issues).

Regarding custody, these uncertainties have a great impact on cross-border issues, namely in terms of respective liabilities and settlement finality. It might often be unclear whether the Settlement Finality Directive applies to a given situation or not, depending on the token's characterisation as a financial instrument or not.

Having a single definition of securities tokens at the European level would help in the development of a cross-border European market.

Question 60. If you consider that the absence of a common approach on when a security token constitutes a financial instrument is an impediment, what would be the best remedies according to you?

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

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

60.1 Is there any other solution that would be the best remedies according to you?

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

We think that it would be more efficient to set up a European definition of what is a security token rather than changing the existing set of rules.

Guidelines could be provided in addition.

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.

We do think that the existing financial instruments regulation under MIFID II should not be changed since it has proved to be efficient. There is no unified definition of financial instruments in EU law and harmonizing

the definition of certain financial instruments in the EU is a complex task as some financial instruments are specific to some jurisdictions only.

We believe that the European Commission should adopt a binding definition of what a security token is in order to create at least a basic level playing field. A definition of a “token” would also be beneficial.

An additional EU guidance on how to characterize security tokens would be useful since it constitutes a first step in the creation of binding rules. Guidance would be helpful in understanding if a security token constitutes a financial instrument and would go some way preventing structuring of security tokens to fall just outside the perimeter.
But creating binding rules ex-nihilo would not be the best approach as we still need to carry out experiments through a sandbox approach.

At the same time, regulation must not leave too much discretion to national authorities, as it could result in divergent approaches between jurisdictions, increasing the risk of regulatory arbitrage.

Question 61. How should financial regulators deal with hybrid cases where tokens display investment-type features combined with other features (utility-type or payment-type characteristics)?

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

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

61.1 Is there any other way financial regulators should deal with hybrid cases where tokens display investment-type features combined with other features?

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

We would like to preserve a hybrid token category. According to its main attributes, it should be classified on case-by-case basis as security or other.

61.2 Please explain your reasoning for your answer to question 61:

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

1) A particular category of 'hybrid tokens' should exist :

Hybrid tokens are incorporating both features of security tokens and features of utility tokens (or other), making them different from a pure type of token. Therefore a particular category should exist for hybrid tokens.

2) A case-by-case approach is preferred :

As such, several different types of hybrid tokens may exist. In some cases, the financial feature of the token may be dominant while in other products, the utility (or other) part may prevail.

The wide variety of those products should be taken into account, and as of today a case-by-case approach may offer the best way of considering these differences.

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.

Current regulation may be globally applicable in its main principles. MIFID II requires entities providing investment services in the EU to be regulated as investment firms. We find it difficult to apply this to persons participating in a DLT for the following reasons:
(1) as DLT platforms may be decentralized, they are not operated by one single entity that can be regulated ;
(2) trading occurring on the DLT is on a peer-to-peer basis, which means that all members of a DLT platform where security tokens are offered are virtually carrying out an investment activity or providing investment services (e.g. dealing on own account or execution of orders).

Services to EU located issuers of security tokens seems less of a concern as the service of placement will be triggered where a firm is arranging the security token offering.

A way of addressing these issues could be twofold : (1) EU regulation to require that security tokens issued by EU entities or issued to fund projects located in the EU to be admitted for trading only on DLT platforms that are set up and operated or on platforms for which settlement is performed by EU investment firms, and (2) to secure the peer-to-peer model, any person can be granted access to the platform, subject to chaperoning rules whereby EU investment firms (or equivalent) would sponsor access of unregulated persons to the platform and perform KYC. This should resolve the concern that unregulated non-EU entities may otherwise provide investment services in the EU on security tokens. Non-EU investment firms accessing the platform via such a sponsored access will be allowed to deal on own account only. They should not be entitled to execute for third parties or to perform other investment services on security tokens. The content of EU regulation should essentially be constructed to address issues of operating on permission based DLT platforms leaving aside permission less DLT.
These may be the basis for the sandbox test.

The existing rules need to be adapted to take into consideration the specificities of the DLT.

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.

MiFID rules and requirements were not formulated with crypto-assets in mind. Clarification is needed on how they translate in relation to DLT/security tokens, especially which actors in the DLT scenario should be subject to authorization/required to comply with MiFID. Another issue is at what point cryptocurrency activity comes within the scope of EU law, this is especially unclear on decentralized platforms like crypto. The goal being to enable the creation of a same level playing field for all actors on the market.

If we adopt the sandbox approach, we should have a European framework with some EU guidance and a NCA practice.

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.

Financial services providers on digital assets are required to register with the French market authority. This NCA approach should be set as guidance overall at EU level, since Financial services providers on digital assets should be registered within national authorities.

Having a European minimum level playing field with a set of rules to ensure control of these operators would help preventing cross-country customer abuses.

New functions exist in the DLT, such as miners, ledger holders, etc. New rules should apply regarding these functions, and especially KYC/AML and localization of minors regarding countries under embargo.
We have to take into account these specificities while setting up the regulatory framework for security tokens. A specific regulatory frame for the Security Tokens should be set up to take into account the specificities of this instrument.

The service of safekeeping and administrating financial instruments for the account of clients, including custodian and related services, should be clearly defined. A European status and passport for custodians of crypto-assets would be very beneficial for the development of DLT ecosystems.

The available definition of "custodian wallet provider" provided in AMLD5 is insufficient and has left too much discretion to Member States in their transposition process, increasing EU fragmentation for this activity.

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.

French national legislation has already been transposing MIFID II into national law.

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

The key issue for the DLT environment is the secondary market.

DLT is a decentralized system and is not compatible with a unique CSD and the principle of a clearing house.

The alternative way is to create some platforms, as suggested, that are used to advertise buying and selling interest without trade execution.

Overall, there might not be any major issues to adapt Trading Venue definitions except CSD, and SFD requirements that will require further review. The fact that trading venues that qualify as MTFs or OTFs under MIFID II are required to be operated by an investment firm remains a key challenge for DLT platforms. But applying trading venue definitions and requirements will increase the regulatory and control frame and avoid all violation of market integrity such as market manipulation.

Some clarifications will be required regarding Share Trading Obligation and Derivatives Trading Obligation, and on which actor is regarded as the “venue” when there is dealing in DLT products.

Distinction between permission based and permission less DLT could be addressed.

1.5. Investor protection

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

Question 67. Do you think that current scope of investor protection rules (such as information documents and the suitability assessment) are appropriate for security tokens? Please explain your reasoning.

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

We assume that this question relates to the situation where an investment firm is providing advice on a client in relation to security tokens. Clarification on other situations when other actors in a DLT scenario could be subject to investor protection rules would be useful.

The set of existing investor protection rules needs to be adapted to the DLT environment.

Information documents should be clear, accurate and sufficiently complete to provide for investors the main information regarding the company and the token and evaluate the different risk towards the investors.

Having a minimum standard for each crypto currency and DLT.

Suitability of products and assessment could be difficult to organize in regard of the variety of security tokens; moreover, setting up too strict rules would restrain market access.

Access to security tokens should be granted to retail but under certain parameters to be determined.

Guidance could be helpful for investors protection and safeguarding rules.

Question 68. Would you see any merit in establishing specific requirements on the marketing of security tokens via social media or online? Please explain your reasoning.

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

The main requirement should be providing a clear list of the different risk factors of the token.

The offering document with a visa of the NCA should be available before the token is advertised on social media.

Each token issued should have a disclaimer that would clearly state that the maximum risk is to lose partially or totally the investment. It should also prominently state the major technological risks inherent to DLT systems.

Clarification could be provided on when marketing of security tokens comes within the scope of EU law.

The disclaimer should be used in each advertisement (even on Facebook, Snapchat, Instagram, Linkedin, Twitter, etc). The disclaimer should also warn the investor that understanding of the token and its risks might require being a usual security tokens investor.

Particular risks associated with security tokens may need to be called out in marketing material.

A suggestion could be to reserve this kind of products to eligible and professionnel counterparts in a first time and to broaden to the retail in the second time.

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.

Tokens are merchandized in a particular way (e.g. Facebook, Twitter) the existence of a specific disclaimer is good. The set of rules used to protect investors should not impede on the development of the new market, but clarity of the disclaimer to mitigate risk taking is essential.

MIFID rules on asset segregation are demanding. The regimes used under French PACTE law (for utility tokens) should be aligned with security tokens, i.e asset segregation between client assets and own assets on the DLT.

The obligation of restitution will need to be adapted.

Key is which actors in a DLT scenario are responsible for the investor protection requirements being applicable, and which member states' laws reflecting MIFID are applicable to a DLT product.

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.

The DTL could offer cost efficiencies to SME Growth Markets, but adapting the current SME growth markets (volume of transactions /speed /etc.) would require big investments.

We cannot properly assess operational issues yet because of a lack of practice.

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

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

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

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

As of today DLT and Blockchains are not MTF. The first step could be to define a status for it.

The DLT system is resilient, we do not see any major issues in applying the requirements to security tokens, but some additional testing is still needed, since it has not been tested whether trading platforms functioning with DLT technology can respond to situations of severe market stress, high volumes of orders, good business continuity. Not sure either that under existing DLT trading platforms algorithmic trading can be controlled adequately, especially regarding its effect on prices.

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.

Currently there is no market and no existing market standards for security tokens. It will be difficult to assess if security tokens should be admitted to trading from an operation point of view.

Market confidence is essential to the development of the security tokens market; therefore adapting the set of requirements of MIFIDs admission rules would be useful.

A sandbox approach could be useful to pursue further assessment.

Question 1.9 Access to a trading venues

In accordance with Article 53(3) and 19(2) of MiFID, RMs and MTFs may admit as members or participants only investment firms, credit institutions and other persons who are of sufficient good repute; (b) have a sufficient level of trading ability, competence and ability (c) have adequate organisational arrangements; (d) have sufficient resources for their role. In effect, this excludes retail clients from gaining direct access to trading venues. The reason for limiting this kind of participants in trading venues is to protect investors and ensure the proper functioning of the financial markets.

However, these requirements might not be appropriate for the trading of security tokens as crypto-asset trading platforms allow clients, including retail investors, to have direct access without any intermediation.

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

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

The market must be open to the retail investors, however strong KYC must be completed in order to ensure security.

The token market must be a broader market constituted by accredited and institutional investors in the first step and opened in a second time to retail.

Requirement of having a sufficient level of trading ability, competence and experience must be adapted to the developing security token market, the contrary would lead to restraining the security token market to institutional investors and qualified investors only, which we do not find appropriate. (Restriction of a regulated security token market would lead the retail investors to participate to private token offerings that are even more risky and uncontrolled; and would close the doors of access to market to a new investor base).

In order to build an open regulated security token market, sufficient levels of transparency, good repute and equal market access must be reached.

If security tokens are admitted for trading on DLT platforms and if such platforms are characterized as trading venues then the MIFID II rules require that they have a regulated operator.

MIFID II provides that an entity that is not an investment firm or a credit institution can be a member of a regulated market or MTF under the following conditions: are of sufficient good repute; have a sufficient level of trading ability, competence and experience; have, where applicable, adequate organisational arrangements; have sufficient resources for the role they are to perform, taking into account the different financial arrangements that the regulated market may have established in order to guarantee the adequate settlement of transactions.

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.

Generally speaking, the DLT environment does not fit to best execution as it is peer-to-peer.

Yet, transparency would be important in a regulated trading venue operated under DLT technology, and should be applied in the use of a in a regulated trading venue.

A careful approach must be taken knowing liquidity must be sufficient and threshold set properly based on the current MiFIR framework.

Most of the exchanges platforms live in an opaque market in particular regarding the trading fees or the bookbuilding process price.

We cannot properly assess operational issues yet because of a lack of practice.
A sandbox approach is needed on this question.

Clarification is probably needed on which actors in a DLT scenario are responsible for complying with the transparency requirements.

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

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

Given that we do not know how the market will be organized, it is very difficult to determine the pre-trade transparency rules (and waivers to those rules) that should apply to it.

Many questions will need to be assessed on a case-by-case basis : orderbook insight to all investors,

including price offered, volume, time of execution, block trades, trading of big orders over smaller once should not provide automatic priority of execution and higher speed.

We cannot properly assess operational issues yet because of a lack of practice.
A careful approach should be taken. Accurate and reliable underlying data to compute relevant transparency threshold and liquidity assessment will be mandatory in order to enforce any transparency requirements if required.

A sandbox approach is needed on this question.

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.

Transaction reporting are not centralized by an investment firm since information is on the DLT system. Moreover a DLT operated regulated trading venue may not have a closing time, it can be operated on continuous bases. MiFIR requirements must be adapted to the DLT environment.

We cannot properly assess operational issues yet because of a lack of practice.

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.

MAR covers insider dealing for security tokens if they meet the definition of a security. Therefore, the scope of article 8 may not be wide enough to capture other types of insider dealing in crypto-assets, e.g. the miners or wallet providers, as provided in ESMA note.

We agree with the assessment that Art 8(4)(c) end of paragraph applies.

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.

MAR is not broad enough to capture all activities and needs to be aligned with the MAR review outcomes and conclusions.

Question 79. Do you think that there is a particular risk that manipulative trading in crypto-assets which are not in the scope of MAR could affect the price or value of financial instruments covered by MAR?

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

Yes, as pointed out in ESMA note. For example, if the underlying of crypto-asset or a security token is a financial instrument covered by MAR as an example of the CFD contracts based on crypto currencies.

Crypto assets could impact MAR instruments and be within scope; crypto assets could be uncorrelated and not captured.

3. Short Selling Regulation (SSR)

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

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

Question 80. Have you detected any issues that would prevent effectively applying SSR to security tokens?

Please rate from 1 (not a concern) to 5 (strong concern)

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

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.

The list of instruments in Annex I of Delegated Regulation 918/2012 would need to be expanded in scope. The list in Annex I does not include a transferrable security but should do so to include a security tokens directly correlated to an equity or sovereign debt.

Security tokens or crypto-assets would need ISINs or a reference to be trackable (similarly to under MiFID II)

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.

Today there is no regulation on platforms regarding assets segregation and margin ratios so it increases risk of platform /investors and an increased market manipulation risk.

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

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

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.

The Prospectus format should be adapted to tokens and to DLT technology.

STOs differ from classical offers covered by Prospectus regulation (audit of smart-contract/ explanation of DLT technology used/ information specific to the token/ segregation / specific risk factors /etc.).

Prospectus regulation currently requires for accounts, results, and forecasts. Companies that are in an early stage cannot provide for such information and will lose the benefits of issuing security tokens if they are required to file a Prospectus in its current format.

4.2. The drawing up of the prospectus

Delegated Regulation (EU) 2019/980, which lays down the format and content of all the prospectuses and its related documents, does not include schedules for security tokens. However, Recital 24 clarifies that, due to the rapid evolution of securities markets, where securities are not covered by the schedules to that Regulation, national competent authorities should decide in consultation with the issuer which information should be included in the prospectus. Such approach is meant to be a temporary solution. A long term solution would be to either (i) introduce additional and specific schedules for security tokens, or (ii) lay down 'building blocks' to be added as a complement to existing schedules when drawing up a prospectus for security tokens.

The level 2 provisions of prospectus also defines the specific information to be included in a prospectus, including Legal Entity Identifiers (LEIs) and ISIN. It is therefore important that there is no obstacle in obtaining these identifiers for security tokens.

The eligibility for specific types of prospectuses or relating documents (such as the secondary issuance prospectus, the EU Growth prospectus, the base prospectus for non-equity securities or the universal registration document) will depend on the specific types of transferable securities to which security tokens correspond, as well as on the type of the issuer of those securities (i.e. SME, mid-cap company, secondary issuer, frequent issuer).

Article 16 of PR requires issuers to disclose risk factors that are material and specific to the issuer or the security, and corroborated by the content of the prospectus. ESMA's guidelines on risk factors under the PR assist national competent authorities in their review of the materiality and specificity of risk factors and of the presentation of risk factors across categories depending on their nature. The prospectus could include pertinent risks associated with the underlying technology (e.g. risks relating to technology, IT infrastructure, cyber security, etc, ...). ESMA's guidelines on risk factors could be expanded to address the issue of materiality and specificity of risk factors relating to security tokens.

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

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

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

schedules for security tokens). Please explain your reasoning.

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

The full prospectus approach is not appropriate for security tokens, for example, the obligation to give three years accounts could be difficult to obtain for a new company, and the requirement is not adapted to developing this ecosystem. We prefer a building block approach to provide information on the token, on the environment of the token (e.g. what kind of DLT is used, the exchange venues for secondary market, the description of the DLT technology, the governance, custodian issue, description of smart contract, audit of the smart contract, use of proceeds may not exactly be the same as in prospectus, etc.)
Information regarding the project, the project governance and management team is essential for the investors. A full description of the company as currently described risks in Prospectus regulation may not be accurate.

The building block approach is necessary to provide for appropriate information.

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

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

No, a specific token ISIN can be created. For example, the “T” could be set before the usual ISIN code.

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.

See response to question 83.

The Prospectus format does not cover adequately such information as technology risk, audit of smart-

contract, DLT technology, information specific to the token, segregation of money deposited, secondary trading, settlement specific to the token (airdrop/ delivery on an account, etc.), custody, etc.

Information requirements in Prospectus regulation specific to the company may not be adapted to early stage companies.

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.

Since the prospectus regulation format as such is not adapted to the token, some specific requirements should be added and other parts alleviated (e.g. accounts / financials).

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.

Disclosure of DLT related risk factors are essential to investor appraisal.

Information should be provided on risks specific to smart-contracts, the DLT used, personal data, segregation of money deposited, secondary trading, settlement specific to the token (airdrop/ delivery on an

account, etc.), custody of tokens, etc.

There should probably be disclosure of more fundamental issues relating to STOs, e.g. whether they are actually share capital, how company and contract law works with them (or areas where it is unclear and not harmonized under EU law).

5. Central Securities Depositories Regulation (CSDR)

CSDR aims to harmonise the timing and conduct of securities settlement in the European Union and the rules for central securities depositories (CSDs) which operate the settlement infrastructure. It is designed to increase the safety and efficiency of the system, particularly for intra-EU transactions. In general terms, the scope of the CSDR refers to the 11 categories of financial instruments listed under MiFID. However, various requirements refer only to subsets of categories under MiFID.

Article 3(2) of CSDR requires that transferable securities traded on a trading venue within the meaning of MiFID II be recorded in book-entry form in a CSD. The objective is to ensure that those financial instruments can be settled in a securities settlement system, as those described by the Settlement Finality Directive (SFD). Recital 11 of CSDR indicates that CSDR does not prescribe any particular method for the initial book-entry recording. Therefore, in its advice, ESMA indicates that any technology, including DLT, could virtually be used, provided that this book-entry form is with an authorised CSD. However, ESMA underlines that there may be some national laws that could pose restrictions to the use of DLT for that purpose.

There may also be other potential obstacles stemming from CSDR. For instance, the provision of 'Delivery versus Payment' settlement in central bank money is a practice encouraged by CSDR. Where not practical and available, this settlement should take place in commercial bank money. This could make the settlement of securities through DLT difficult, as the CSDR would have to effect movements in its cash accounts at the same time as the delivery of securities on the DLT.

This section is seeking stakeholders' feedback on potential obstacles to the development of security tokens resulting from CSDR.

Question 88. Would you see any particular issue (legal, operational, technical) with applying the following definitions in a DLT environment?

Please rate from 1 (not a concern) to 5 (strong concern)

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

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

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.

Custodians holding investor assets work with CSDs to ensure the safe delivery/transfer of assets and funds to each of the respective transacting parties and handle the settlement of transactions.

Part of the complexities in post-trade processes derives from the need of both sides of the trade to maintain records of the information around the transaction and the resulting counterparty risks, and the cost of reconciling each party's data with the data of the counterparty at each step of the contract execution.

The use of the blockchain in post-trade allows for the maintenance of a single, shared, immutable ledger of transaction information that is updated at each step of the process and can be instantly accessed by all involved parties. Therefore, depending on the way DLT environments are shaped, these could exclude the use of CSDs altogether by replacing CSDs by the distributed ledger as a decentralised version of such depositories.
Regarding settlement internalisers, entities could potentially qualify as such in a permissioned DLT environment. However, the opportunity and advantages of doing so remains unclear at this stage.

There are scope questions or items which may need adaptation in a CSDR context:

Could a distributed ledger be a 'securities settlement system' for the purpose of CSDR Article 2(10)? This will only be the case (among other criteria) if:

(a) there are the required number of participants (it is unclear if each DLT participant could be regarded as a "system operator"?) ;
(b) transfer orders can be executed through the DLT ; and
(c) the DLT submits itself to an EU MS law (and it is not clear what law the DLT would be subject to unless MS/ EU law defined this). It will depend on if transfer orders can be effected and whether it is a designated system under any Member State law (among other criteria).

Will securities settlement records continue to be held on DLT or will they continue to be held by the CSD operationally (with the DLT having a mirror record)? There is a need for clarity on which is the authoritative legal record of ownership.

We agree that any legislation will need to define and update 'dematerialised form' as it is unlikely DLT transfers can be deemed to be 'book entries' under Article 2(4).

The scope of Article 9 CSDR would have to be reviewed and updated (internalised settlement reporting) as an institution (e.g. an investment firm) is responsible for reporting transfer orders outside of a securities settlement system and it should be clarified how this relates to DLT providers.

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.

These definitions were not designed with a DLT environment in mind. As such, they are source of regulatory uncertainty unless interpreted in a compatible way with DLT or amended in such a way to adapt to DLT specificities.

As DLT implies decentralization and disintermediation, the above definitions might constitute a regulatory obstacle to the development of DLT environments.

The CSDR entrusts to the CSD a role in operating a system for settlement of the securities recorded on an account in it. If security tokens could be recorded in an account on a blockchain via a CSD, the blockchain in question would also have to be able to be considered as a securities settlement system within the meaning of the Settlement Finality Directive.

In the current state of the legislation, we believe that the complete tokenisation of the settlement and delivery of security tokens is impossible. Although the delivery of security tokens could be performed on a blockchain operated by a CSD authorised for this purpose, settlement, meanwhile, would in theory have to take place in fiduciary money and not in cryptocurrency.

This would require the CSD to effect movements in its cash accounts at the same time as the blockchain, which to some extent limits the productivity gains that can be expected from the tokenisation of post-trade infrastructures. A legislative adaptation of the CSDR seems necessary to allow settlement in cryptocurrency. Conversely, this legislative adaptation would not be necessary if the European Central Bank decided to issue central bank money on a blockchain.

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

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

89.1 Please explain your reasoning for your answer to question 89:

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

We share ESMA’s opinion(*) that the CSDR is not prescriptive regarding the nature of the recording on an account with the central depository. In light of Recital 11 according to which the Regulation does not intend to "impose one particular method for the initial book-entry recording, which should be able to take the form of immobilisation or of immediate dematerialisation", ESMA considers that it is incumbent on national law to indicate the form that could be taken by recording on an account, including on a blockchain. The only constraint imposed by the regulation is that this recording on an account should take place via an authorised central depository.

The CSDR therefore does not oppose the recording of security tokens in the central depository taking place via a blockchain and not via an account as understood from an accounting viewpoint. However, routing via the intermediary represented by the CSD remains an obligation. As things stand at present, a platform listing security tokens should therefore perform settlement and delivery either via another market participant authorised as CSD or by being itself authorised as CSD.

Although some Member States have considered CSDR book-entry requirements compatible with security tokens, what a book-entry system really means in a DLT environment needs some clarification

(*) https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

Question 90. Do you consider that national law (e.g. requirement for the transfer of ownership) or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT solution? Please explain your reasoning.

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

Yes, there are probably clarifications that need to be made in national law to recognize and support DLT solutions. Different jurisdictions are at different stages of considering these issues and the diversity of developments across member states will probably hinder use of DLT.

For example, for company laws, in various jurisdictions, it is unclear whether security tokens are share capital (and which laws and accounting treatment of share capital should apply, or voting or dividend rights), laws on ownership of dematerialized securities and contract laws.

In France, law and regulators facilitate the use of DLT solutions. However, EU financial law prevents them from taking further measures aimed at promoting DLT use in financial services. As such, regulatory flexibility with respect to targeted EU rules hindering the development of DLT ecosystems at national level (e.g. through an exemption/sandbox mechanism) is needed.

Question 91. Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment?

Please rate from 1 (not a concern) to 5 (strong concern)

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

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.

It is likely that these obligations will have to be adapted to allow for the specific characteristics of the blockchain for which technology is likely to ensure greater security in transactions than routing via a regulated intermediary (the settlement discipline and issuance integrity rules could, for example, prove superfluous). Apart from the costs, these requirements appear inappropriate for the way in which the blockchain operates (unfalsifiable distributed ledger, smart contracts).

Question 92. In your Member State, does your national law set out additional requirements to be taken into consideration, e.g. regarding the transfer of ownership (such as the requirements regarding the recording on an account with a custody account keeper outside a DLT environment)? Please explain your reasoning.

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

6. Settlement Finality Directive (SFD)

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

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

Question 93. Would you see any particular issue (legal, operational, technical) with applying the following definitions in the SFD or its transpositions into national law in a DLT environment?

Please rate from 1 (not a concern) to 5 (strong concern)

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know / no opinion / strong concern
Definition of a securities settlement system	○	◉	○	○	○	○
Definition of system operator	○	○	○	◉	○	○
Definition of participant	○	○	○	◉	○	○
Definition of institution	◉	○	○	○	○	○
Definition of transfer order	○	◉	○	○	○	○
What could constitute a settlement account	○	○	◉	○	○	○
What could constitute collateral security	○	○	◉	○	○	○

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.

Yes - it is generally unclear how to identify which of the participants in a DLT environment definitively fall under the definitions, e.g. system operator.

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.

Identification of a securities settlement system manager for the purpose of authorisation by the central securities depository seems incompatible with decentralised platforms or platforms operating on a public blockchain.

Question 94. SFD sets out rules on conflicts of laws. According to you, would there be a need for clarification when applying these rules in a DLT network (in particular with regard to the question according to which criteria the location of the register or account should be determined and thus which Member State would be considered the Member State in which the register or account, where the relevant entries are made, is maintained)? Please explain your reasoning.

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

In our opinion, the main issue here relates to public blockchains. In this case, determining where the account is located can prove difficult. Clarifications on this aspect would be beneficial.

Regarding, private blockchains, the place of registration of the blockchain could be a criteria compatible with SFD.

The SFD is implemented nationally by the member states, but it is not clear, as with much of DLT which member state has jurisdiction as to ownership and settlement finality, not to mention unclear when a DLT is actually within the scope of EU jurisdiction.

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.

In this regard, in France, the law retained is the one of the state where the account is maintained.

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

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

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

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

The obligation of intermediation to take part in a securities settlement system is an obstacle to the effective functioning of a DLT solution.

The identification of a securities settlement system manager for the purpose of authorisation by the central securities depository also seems incompatible with decentralised platforms or platforms operating on a public blockchain.

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[32].

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

Question 97. Would you see any particular issue (legal, operational, technical) with applying the following definitions in the FCD or its transpositions into national law in a DLT environment?

Please rate from 1 (not a concern) to 5 (strong concern)

	1 (not a concern)	2	3	4	5 (strong concern)	Don't know / no opinion / strong concern
If crypto-assets qualify as assets that can be subject to financial collateral arrangements as defined in the FCD	◉	○	○	○	○	○
If crypto-assets qualify as book-entry securities collateral	◉	○	○	○	○	○
If records on a DLT qualify as relevant account	◉	○	○	○	○	○

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.

Some issues include:

- the segregation of the collateralized token ;
- the use of smart contract technology in order to secure the collateral ;
- the existence of a legal framework that will allow collateralizing tokens ;
- in the use of smart-contracts in that legal framework

There are various definitions which need to be reviewed and possibly clarified as to how to DLT. However they go beyond matters of law covered by the FCD. They concern various company, insolvency law and property law concepts referred to in FCD definitions where it isn't clear how they apply to DLT - e.g. "winding up procedures", "financial instruments", "cash", etc.

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[32]?

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

The main issue here relates to public blockchains. In this case, determining where the account is located can prove difficult. Clarifications on this aspect would be beneficial.
Regarding, private blockchains, the place of registration of the blockchain could be a compatible criteria.

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.

In this regard, in France, the law retained is the one of the state where the account is maintained.

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.

If security tokens qualify as transferable securities and are traded on a regulated market, they will have to be recorded with an authorized CSD.

As a DLT is mostly a peer-to-peer, it seems that there is no need for Central Clearing as traded on DLT. The delivery guarantee is provided by the DLT. Significant efficiency gains in post- trade could be achieved through tokenisation. Post- trade comprises the settlement, custody and, optionally, clearing of securities. In this area, the processing of securities transactions should also be simplified and accelerated by the improved data quality and the omission of intermediaries.

Question 102. Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment?

Please rate from 1 (not a concern) to 5 (strong concern)

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

						strong concern
Rules on margin requirements, collateral requirements and requirements regarding the CCP's investment policy	○	○	○	○	○	◉
Rules on settlement	○	○	○	○	○	◉
Organisational requirements for CCPs and for TRs	○	○	○	○	○	◉
Rules on segregation and portability of clearing members' and clients' assets and positions	○	○	○	○	○	◉
Rules on requirements for participation	○	○	○	○	○	◉
Reporting requirements	○	○	○	○	◉	○

102.1 Is there any other particular issue (including other provisions of EMIR, national rules applying the EU acquis, supervisory practices, interpretation, applications, ...) with applying the current rules in a DLT environment? Please specify which one(s) and explain your reasoning:

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

102.2 Please explain your reasoning for your answer to question 102:

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

Tokenisation in the settlement of payment transactions will primarily affects securities settlement. It will be very difficult to apply some rules on Settlement

As the complexity of such transaction they have to be reported.

Ideally, it is expected that issuers and investors would be able to conclude transactions with each other directly without intermediation by other participants, such as central securities depositories (CSDs) or custody banks. The long custody chains that are typical in securities business at present could then be shortened considerably. The resulting leaner processes in post- trade would likely lead to efficiency gains and cost savings. In addition, smart contracts are well suited to settling various corporate actions (e.g. coupon payments) in a more efficient way. Some steps in the process could be automated and the need for reconciliation as well as the number of errors arising from the reconciliation process are likely to decrease as a result of common data storage.

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

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

Yes Tokenisation allows for extensive digitalisation in the settlement of payment transactions so that, in several cases, confirmations and reconciliation processes can be carried out more quickly and some steps in the process chain can even be omitted entirely
Indeed, some of the issues that CCPs and TRs aim to tackle might already be solved within DLT solutions. It must be carefully assessed whether and when the use of CCPs and TRs may be warranted, necessary or redundant in a DLT environment.

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

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

No, as derivatives are financial products they have to follow the existing rules.

9. The Alternative Investment Fund Directive

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

The following questions seek stakeholders' views on whether and to what extent the application of AIFMD to tokens could raise some challenges. For instance, AIFMD sets out an explicit obligation to appoint a depositary for each AIF. Fulfilling this requirement is a part of the AIFM authorisation and operation. The assets of the AIF shall be entrusted to the depositary for safekeeping. For crypto-assets that are not 'security tokens' (those which do not qualify as financial

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

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

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

	1 (not suited)	2	3	4	5 (very suited)	Don’t know / no opinion / very suited
AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;	◉	○	○	○	○	○
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;	○	○	◉	○	○	○
Employing liquidity management systems to monitor the liquidity risk of the AIF, conducting stress tests, under normal and exceptional liquidity conditions, and ensuring that the liquidity profile and the redemption policy are consistent;	○	○	○	○	○	◉
AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets;	○	○	○	◉	○	○
Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments.	○	○	○	◉	○	○

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.

In regard of French regulation for example, when an AIF fund or an OPCVM invests in financial instruments (in the future perhaps security tokens) registered in DLT, the registration is done in a registered (nominative) form and is impossible if bearer form should be used. An evolution is wished in regard of registered form of registration. It would be needed that bearer form could also be applied in the frame of DLT registration.

In French law when registration of financial instruments is made in registered form the FIA or the OPCM that is keeping the register is only responsible for the registration and not for the safekeeping. In case of loss of the financial instruments there is no obligation to return the financial instruments to the investor.

A change in law to apply bearer form in DLT will allow for a more complete investor protection.

In regard of passive fund investing the liability of the various actors is also a question, e.i. hybrid liability holding with on one side a part of register on a DLT and on the other side the second part of the registry in a traditional kind of registry. What would be the interoperability between the actors linked to collection of orders, subscription, redemption of UCI units, central depository of the security tokens etc.

What are the frames of management companies due diligence and duty of care as services provider in DLT environment, and how does it translate into liability? How should passive record keeping be treated in DLT?

Other considerations are the issue of delivery of cash. Currently cash delivery is an impediment to the development of crypto-assets in asset management. Having a stable coin or another type of bridging tool is necessary for future development.

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.

Regarding investment funds for which we act as a depositary, there are many unanswered questions regarding our liability and the restitution obligation in case of loss of assets.

We are in favor of the approach taken by France on digital assets in its PACTE law which is that in any case, the depositary of crypto-assets (e.g. security tokens) should not be responsible for the restitution of the underlying assets but for the restitution of the means of access to said assets. The restitution obligation should only apply to the private keys as the depositary has no control over the underlying assets themselves.

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

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

106.1 If you do consider that the effective functioning of DLT solutions and/or use of security tokens is limited or constrained by any of the AIFMD provisions, please provide specific examples with relevant provisions in the EU acquis. 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 105.2.
Relevant EU provisions include art. 21 (12) of the AIFMD.

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

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

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

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

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

	1 (not suited)	2	3	4	5 (very suited)	Don't know / no opinion / very suited
Provisions of the UCITS Directive pertaining to the eligibility of assets, including cases where	○	○	◉	○	○	○

such provisions are applied in conjunction with the notion “financial instrument” and/or “transferable security”						
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;	○	○	○	○	○	◉
UCITS Directive rules on the arrangements for the identification, management and monitoring of the conflicts of interest, including between the management company and its clients, between two of its clients, between one of its clients and a UCITS, or between two -UCITS;	○	○	○	◉	○	○
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.

Regarding investment funds for which we act as a depositary, there are many unanswered questions regarding our liability and the restitution obligation in case of loss of assets.

We are in favor of the approach taken by France on digital assets in its PACTE law which is that in any case, the depositary of crypto-assets (e.g. security tokens) should not be responsible for the restitution of the

underlying assets but for the restitution of the means of access to said assets. The restitution obligation should only apply to the private keys as the depositary has no control over the underlying assets themselves.

As such, article 24 of the UCITS regulation does not seem fully compatible with a DLT environment

11. Other final comments and questions as regards tokens

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

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

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

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

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

An experimentation framework must be established at EU level to allow targeted regulatory requirements to be lifted for selected projects so that they can in turn develop in a regulatory certain environment, with proper governance and oversight arrangements.

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

110.1 If you do 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, please identify the issues that should be addressed at EU level and the approach to address them. Please explain your reasoning.

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

Question 111. Have you detected any issues beyond those raised in previous questions on specific provisions that would prevent effectively applying EU regulations to security tokens and transacting in a DLT environment, in particular as regards the objective of investor protection, financial stability and market integrity?

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

111.1 Please provide specific examples and explain your reasoning for your answer to question 111:

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

We see some issues:

- in transparency requirements application in their current state ;
- the replication of prospectus publication requirements that would not be adapted to the DLT specific framework ;
- in the replication of ISIN/ CSD and settlement obligations, since DLT technology does not use a central intermediary.

As a general comment we believe that in several regards a sandbox approach would be preferable since there is not enough distance to assess the overall impacts of transposing existing regulation to the DLT framework.

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.

In France the national regulators have started setting up a sandbox approach :

- PACTE law has been creating a first framework for the use of DLT ;
- The Financial Authority (AMF) has been setting up a specific regime dedicated to utility tokens, providing for an optional visa for ICO issuings.

Existing national rules on AML-CFT provisions also raise issues when dealing with miners on a public (e.g. where the miners are established in sanctioned countries for instance, and are remunerated through the DLT protocol).

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.

The regulation of electronic money does not take into account the possibility for holders of electronic money to transfer it to other holders without the intermediation of the electronic money issuer (or another regulated entity).

If a crypto-asset which qualifies as electronic money is based upon a public blockchain protocol (e.g. Ethereum-based stablecoins), then the issuer would not be able to control the transfer and the use of its electronic money.

Quasi-financial services using stablecoins have emerged over the last year and allow, for example, to earn interest by depositing stablecoins or to borrow stablecoins. Article 12 of the EMD2 prohibits "the granting of interest or any other benefit related to the length of time during which an electronic money holder holds the electronic money."

Therefore, the EMD2 should be updated to take into account the fact that e-money tokens are able to be transferred "peer-to-peer", provided that it is possible to identify the beneficiary of the operation and the traceability of movements of funds (AML5 issue).

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.

Although the issue outlined above still applies in relation with PSD2, the fact that individuals and companies may transfer e-money tokens (i.e. stablecoins which qualify as electronic money) in a peer-to-peer way should not prevent the effectiveness of the payment services regulation.

In any case, payment institutions which would open e-money tokens accounts or realize payment transactions in relation with e-money tokens should remain within the scope of PSD2 and apply the strong authentication requirements (transfer is a payment).

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.

As explained above, legal amendments and supervisory guidance would be needed at least to clarify the application of EMD2 and PSD2 to stablecoins which qualify as electronic money.

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

Question 116. Do you think the requirements under EMD2 would be appropriate for "global stablecoins" (i.e. those that reach global reach) qualifying as e-money tokens?

Please rate from 1 (completely inappropriate to 5 (completely appropriate)

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

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.

- Initial capital and ongoing funds : method D of Article 5 of EMD2 provides that the own funds of an electronic money institution shall amount to at least 2% of the average outstanding electronic money.

- Safeguarding requirements : Global stablecoins issuers should be able to invest funds received in exchange for electronic money in "secure, low-risk assets" mentioned in Article 7(2) of EMD2.

- Redeemability : Global stablecoins scheme may be more efficient if redemption rights are limited to authorized intermediaries.

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.

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

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

117.1 Please explain your reasoning for your answer to question 117:

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

Additional information

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

The maximum file size is 1 MB.
You can upload several files.
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

Useful links

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

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

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

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

Contact

fisma-crypto-assets@ec.europa.eu