Contribution ID: a3f6370b-f440-4895-8564-5f306a858618
Date: 01/04/2020 18:12:38

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

Julian

* Surname

SCHMÜCKER

* Email (this won't be published)

j.schmucker@ebf.eu

* 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

European Banking Federation

* 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.

4722660838-23

* 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:

European business association

* 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.

DLT and its subset blockchain technology pose a great opportunity to develop new innovative services as well as to increase the efficiency, level of security and competitiveness of financial services.

With technological developments still ongoing, the ultimate effect of DLT based solutions cannot be pinpointed with all certainty today. However, what already became clear is the challenge posed by the widespread mix of terminology when addressing the topic in the first place. A distinction of crypto-assets from other terminology such as crypto-currencies and digital assets is important to understand the appropriate approach to the targeted asset, the technological implications and the regulatory solutions suitable to address them.

For banks, it is essential to understand the regulatory implications of crypto-assets. In order to have sufficient legal certainty, the applicability of EU legislation to crypto-assets is key to assess and potentially incorporate this new technology into existing processes of European banks.

To provide for an efficient consultation tool, the EBF supports the crypto-asset target of this initiative. Moreover, to build a fully-fledged regulatory framework, regulators should also take into account the specificities relating to market participants, market infrastructure and consumer protection.

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.

A uniform legal definition at the EU level can help to ensure a common regulatory approach to crypto-assets in different member states. More homogeneous considerations under the applicable legal framework can support legal certainty, advanced stakeholder protection, a European level playing field and the general ability of market participants to scale-up solutions to the European level. These factors can ultimately contribute to a stronger European positioning at the global level in terms of technological innovation and its economic application. That is why European banks support a pan-European approach rather than multiple national regulatory frameworks creating de facto an unlevel-playing field.

Cryptographic tokens running on DLT systems could soon form an integral part of various major economic sectors (e.g. financial markets, information and media, manufacturing and trade). As such, they are going to provide utility and value in many different forms to business and society as a whole. Moreover, cryptographic tokens are also on the verge of representing a recognized institutional asset class. Yet, the current token markets still lack a tangible and holistic framework for the identification, classification and analysis of different token types, which leads to economic, technological as well as regulatory uncertainty and a lack of transparency for all players involved. With the objective of addressing some of these shortcomings, public and private initiatives such as DIN/ISO or the International Token Standardization Association (ITSA) may help to implement comprehensive market standards for the global token economy.

Both regulation and supervision should properly address characteristics and risks of crypto-assets. A classification can support the central assessment for each crypto-asset in terms of applicable regulation. While not all assets will require a regulatory response by additional legal requirements (e.g. security tokens being classified as financial instruments under existing regulation), others may not fit into the existing framework.

Generally, regulation will need to be able to respond quickly to future, new categories of crypto-assets when they will arise. A classification will help to support these future adaptions, providing a legally certain foundation for regulatory assessments.

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 conversation around individual classifications is ongoing. A clear taxonomy can help to differentiate among crypto-assets. Based on such differentiation, the regulatory treatment could consider more appropriately the particular risks involved. This could help legal clarity, and to develop an appropriate oversight approach, while leveraging the benefits of a global coordination.
Fundamentally speaking, the classification of crypto-assets should relate to the economic function of the asset, meaning a close understanding of the actual use of the token. Additionally, the factors of intrinsic value and associated rights must be considered. This is closely related to the specific risks of the asset, possible influenced by the existence of an identifiable issuer, the enforceability of the proclaimed rights or the underlying source of value. Future regulatory classification may require a regular review and update, as the technological advances and market environment evolves. A flexible fit-for-purpose classification is required.
The codification of classifications requires a continuous discussion with European banks. Reflecting non-exhaustive considerations up to now, the following classes can provide guidance for future exchanges:

- Crypto-Assets: Digital assets which utilize cryptography and distributed ledger technology (DLT). It's an umbrella term including Security Tokens, Utility Tokens and Payment Tokens.
- The term "token": A digital representation of value, whose ownership is recorded on a distributed ledger that is controlled by cryptographic keys. Having the private key shows ownership of a token. There are three major types of tokens, based on their economic function:
  - Security Tokens (equity and debt tokens, investment tokens) are crypto tokens issued to investors in a token sale or security token offerings (STO) for the exchange for fiat money or other cryptocurrencies. When purchasing Security Tokens, the investor expects a future cash flow, and hopes to generate a capital gain when selling them. To be considered as a "financial instrument". However, not all investment tokens are automatically security tokens.
  - Utility Tokens enable access to a specific product or service often provided using a DLT platform but are not intended to be accepted as a means of payment for other products or services. Utility tokens allow interaction between the users and the company through a platform, for example incentivizing transaction validation.
  - Payment Tokens are used as a means of exchange, replicating the functionality of a coin. Primary purpose is to make peer-to-peer payment. Different sub-types of Payment Tokens exist.
    i. "Cryptocurrency" is a Payment Token which is secured using cryptography. The individual Crypto Coin fluctuates in value, since it is not being kept stable (e.g. Bitcoin or Litecoin). It is negotiable and convertible into legal tender (fiat money).
    ii. "Stablecoin": a cryptocurrency that is pegged to another asset, of which value is kept stable. This can be stable by putting all collateral in another asset (fiat currencies) or pool of assets, or stable by putting collateral in other crypto-currency and that an algorithm keeps the value pegged to another asset (fiat currencies).
    iii. Asset-backed Commercial Bank coin: a DLT representation of money issued by a commercial bank.
    iv. Central Bank Digital Currency (CBDC): a liability of a central bank withdrawable for cash at par.

Looking at these classes, the continuous discussion can note three broad categories:

- Native crypto-assets ("cryptocurrencies")
- Price-stable crypto-assets (generally used for payments). This includes Central bank digital currency (CBDC), depository coins (fiat-linked issued by a commercial bank), FMI tokens (tokenized payment system), and stablecoins.
- Security tokens (falling under the definition of security or other financial instruments under existing EU legislation, since they inherit the respective characteristics)

Reflecting technological developments, two additional categories, possessing their own set of characteristics, can be discussed:

- Non fungible tokens (e.g. digital collectibles or digital art)
- Distributed application (or dApp) tokens (a special token that is issued on top of an existing network

whose function is to allow usage or governance of a particular distributed application). In some respects, these tokens might behave as prepaid API keys or voting tokens.

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.

European banks support a continuous engagement with regulators to enable an advanced understanding on all sides of factors necessary for the distinction.
The potential use or economic function of the token are essential for its distinction. The latter can help framing the classification of crypto-assets. However, additional criteria for classification come into play as well. Intrinsic value and associated rights must be considered. This is closely related to the specific risks of the asset, possible influenced by the existence of an identifiable issuer, the enforceability of the proclaimed rights or the underlying source of value.
Should a classification be limited to a token distinction only, the protection of nominal value (e.g. for holders of asset-backed stablecoins; but not for broader cryptocurrencies) would not be sufficiently recognized.

Furthermore, categories related to the economic function may not be mutually exclusive, since a token can show hybrid features of different financial instruments or evolving features. In this case, tokens that do not fit completely into a regulated category instrument would require a case-by-case approach. Guidance on the appropriate treatment of such assets would be necessary.

Reflecting considerations up to now (see also answer to Q.7), the following types of tokens can nevertheless provide guidance for future exchanges as part of a wider, more aware consideration:
o Security Tokens (equity and debt tokens, investment tokens) are crypto tokens issued to investors in a token sale or security token offerings (STO) for the exchange for fiat money or other cryptocurrencies. When purchasing Security Tokens, the investor expects a future cashflow, and hopes to generate a capital gain when selling them. To be considered as a "financial instrument". However, not all investment tokens are automatically security tokens.
o Utility Tokens enable access to a specific product or service often provided using a DLT platform but are not intended to be accepted as a means of payment for other products or services. Utility tokens allow interaction between the users and the company through a platform, for example incentivizing transaction validation.
o Payment Tokens are used as a means of exchange, replicating the functionality of a coin. Primary purpose is to make peer-to-peer payment. Different sub-types of Payment Tokens exist.
o Hybrid tokens (e.g. Ether) are utility tokens that are needed to record transactions on the respective ledger but could also be a security token when it was issued.

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.

In the understanding of the European Banking sector, different value chains and models for each of this type of crypto assets will emerge. Hence, they will need to rely on different regulatory and supervisory practices.

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.

Reflecting the different market observations in Member States by EBF members, the consideration of crypto-assets as deposits require further observation and exchange.

While crypto-assets (as currently marketed) should not be considered as deposit, certain stablecoins – backed by funds segregated in bank accounts – could gain relevance as e-money, thereby being subject to the EMD. To understand when such as constellation may be applicable, careful consideration must be given to the issuer and backing of the stablecoin (commercial banks' role). In this regard it is important to stress that banks, being experienced to operate in essential compliance with the applicable set of prudential rules, are in the best position to look at deposit-guaranteed digital currencies. Banks already use technological solutions (core bank systems) to record deposits on behalf of clients. It is quite possible that these core bank systems become DLT connected or enabled (or indeed DLT-based) over time. To that extent it is possible to evidence bank deposits in a DLT.

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.

Considering the existing funding channels provided for by financial institutions within the traditional environment of the financial sector, crypto-assets' potential can be considered when looking for complementary ways to create funding for entities that find it difficult to obtain capital in this ecosystem.

For such entities, the new technology may offer an enhanced financial inclusion. Costs in fundraising can be reduced and the speed of negotiations for contracts possibly be increased, for instance allowing for almost real time transaction while reducing complexity of reconciliation processes. For these reasons ICOs and STOs could be a useful and convenient fundraising source for start-ups and early-stage companies, but also a new investment opportunity for investors. As ESMA observed "ICOs could provide a useful alternative funding source for blockchain start-ups and other innovative business that would find it difficult to raise capital through traditional funding channels" (advice "initial coin offerings and crypto-assets", 9 January 2019).

Leveraging the DLT-based potential of crypto-assets, smart contracts offer the possibility of automated execution of contracts.

DLT-based markets enable the technological possibility to consider embedded supervision. Real-time monitoring of transactions or transformed data collection exercises by public authorities open the door to a discussion of enhanced supervisory capabilities. Such discussion would aim for increased efficiency of reporting by financial institutions.

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.

It is important to acknowledge that many means of funding already exist in the current financial system. Additionally, crowdfunding is receiving a pan-European regulatory framework. Generally speaking, a new asset class needs appropriate infrastructure.

To this extent, it should be considered that market participants will sustain certain initial costs before reaching full market potential, thus benefitting from cost reductions. Markets for dealing in crypto assets will most likely see the initial surge of many initiatives, albeit only a few will eventually stabilize.

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.

Crypto-assets have an international impact, challenging multiple jurisdictions with uncertainty in terms of applicable regulation. The token economy operates cross-border, in turn triggering potentially different regulatory and supervisory approaches in multiple jurisdictions. European banks consider enhanced cross-border cooperation of regulators and stakeholders to be an important step to address the risk of regulatory fragmentation as well as the individual risks laid out under question 11.

Operating in an environment of legal uncertainty for treatment of crypto-assets, financial institutions are significantly challenged to understand the necessary compliance when interacting with crypto-asset providers or when determining the effect on/chances for the existing business models of European banks. Risks related to crypto-assets can depend on the characteristics of each token. While for a potentially global stablecoin, financial stability or monetary policy transmission risks may be particularly significant, in the case of a utility token consumer protection risks could be more relevant.

Additional to the required legal clarity in terms of applicable consumer protections rules, crypto-assets can make it difficult for consumers and investors to understand the financial significance of the product in question. Risks are not properly disclosed, potentially creating a false sense of consequences by the investment/purchase decision.

We like to highlight particular risk:
- Extreme volatility and speculation, including the risk of total loss of the investment
- Misleading disclosure of information to consumers
- Lack of liquidity and price transparency
- Scarcity of reliable exchanges

As DLT is the underlying technology of crypto-assets, there are wider questions in terms of data protection, raising the issue of DLT interaction with the GDPR. For example, the GDPR is based on an underlying assumption that in relation to each personal data point, there is at least one natural or legal person (the data controller) whom data subjects can address to enforce their rights under EU data protection law. Decentralized technologies may diffuse or confound responsibility and accountability, which can be challenging in systems that are permissionless or where participants remain anonymous.

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.

European banks support the careful attention that the European Central Bank and EU institutions are paying to the risks of crypto-assets, e.g. in terms of implications for the monetary policy. In an extreme scenario, if euro cash and electronic payment instruments hypothetically gave way to crypto-assets for retail payment transactions, there could be significant implications for monetary policy and economic activity.

Exploratory work of the ECB – though targeting cryptocurrencies and not all suggested classifications under Q.7 - identified relevant risk considerations:

- Crypto-asset risks originate from:

i) the lack of an underlying claim
ii) their unregulated nature outside of the definition as financial instrument or e-money
iii) the absence of a formal governance structure.

- crypto-asset risks depend on their interconnectedness to economy:

i) holdings of crypto-assets without requirements of institution types or bank account
ii) investment vehicles
iii) retail payments

Potentially large and unhedged exposures of financial institutions to crypto-assets could have financial stability implications, all the more so since there is currently no identified prudential treatment for crypto-asset exposures of financial institutions.

Regarding taxation, custodians of crypto values and wallet operators should have the same obligation as credit institutions, i.e. they should also be obligated to without capital gains tax under tax law when trading cryptocurrencies.

Finally, financial market infrastructures (FMIs), particularly payment systems, securities settlement systems and central counterparties, carry the risks of crypto-assets and may act as channels for the transmission of these risks through the financial system. First, financial market infrastructures may be exposed to risks from their participants' crypto-asset activities to the extent that adverse crypto-asset market conditions or other adverse events may compromise participants' ability to meet their obligations. In this case, crypto-asset market-based shocks could be passed from one participant or infrastructure to another/others. Second, financial market infrastructures may pose risks if they clear high risk crypto-asset-based products or use high risk crypto-assets for settlement, collateral or investment.

"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.

Programmable digital money is an innovation with potential that could be a central component in the next stage of the evolution of digitalization. Public authorities recognize that stablecoins offer an alternative that can be used for making payment transactions. Unlike other types of crypto-assets, whose value can fluctuate significantly, stablecoins aim to stabilize their value making them more suitable to serve as a store of value and means of payment. As the G7 report on stablecoins pointed out, stablecoins offer new opportunities to increase the efficiency of the payment system and could potentially contribute to the development of global payment arrangements that are faster, cheaper and more inclusive.

However, banks continue to play an important role in a financial ecosystem utilizing Distributed Ledger Technology, including stablecoins. Operations utilizing stablecoin solutions will require an infrastructure to run processes such as identity solutions, data management and settlements. Picturing a possible interconnected environment using stablecoins in relevant data ecosystems – for example health and mobility sectors – customers require a layer of trusted services. Banks have a long tradition of providing safe and reliable services to customers, combining a sound understanding of security, customers' need and reliability. Hence, banks are the ideal operator to provide the trusted service layer in an DLT environment using digital money.

The European banks call upon the ECB to actively engage in the process of assessing and understanding the impact of a European digital currency. Europe's position as a digital leader and the European economy's ability to utilize opportunities of digital innovation depend on the possibility to leverage digital currency. Mindful of the fast-evolving technology behind this discussion and possible implications of privately controlled digital currency projects, European banks recommend to carefully evaluate possible options for private initiatives issuing digital currencies in a central bank-controlled environment.

Any stablecoin arrangement has the potential to become global. Therefore, it appears not recommendable to distinguishing between 'stablecoins' and 'global stablecoins' per se. Instead, a discussion could distinguish between 'stablecoins' and 'systemically important stablecoins', i.e. those stablecoins that have the propensity to impact global financial stability. Crypto-assets in general can be considered global due to their digital nature. Focus should be on the potential impact of the individual initiative for the financial system or the economy, e.g. due to its potential reach (e.g. when sponsored by large technology or financial firms with a large customer base).

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.

In line with positions issued by EU institutions in 2019, stablecoins may present changes for payment processes, targeting a cross-border payments field (see joint statement by the Council and the Commission on stablecoins, 5 December 2019). However, these opportunities need to be considered in light of the connected “multifaceted challenges”, as pointed out by Council and Commission. The EBF welcomes the EU institutions’ awareness, and encourage a thorough assessment, targeting a financial system that operates on the principle “same services, same risks, same rules”. European banks believe that these private stablecoins initiatives, if used for payment transactions, should face the same scrutiny as any other payment product. When it comes to security and customer protection as stipulated in PSD2, data privacy as stipulated in the GDPR as well as requirements related to AML, KYC, ATF and other legal requirements, a level playing field must exists between all payment products. All payments providers should be subject to comparable supervision and regulation.

In the European context, cross-border payments are already well developed and regulated, and instant cross-border payments are expected to become a reality shortly. Global stablecoins may offer another effective technology to facilitate cross-border payments, if an appropriate regulatory and supervisory framework is ensured to address risks stemming from these initiatives, while avoiding hampering innovation in payments. We believe that ensuring a common understanding on these initiatives and globally consistent response from authorities is key due to the cross-national nature of most of this payment initiatives.
In addition, any payments platform that becomes a systemically important financial markets infrastructure should be regulated and supervised as such to safeguard financial and economic stability. Given the propensity of platforms to dominate in their respective spaces, we risk creating a too-big-too-fail payments provider without appropriate oversight, regulation and backstops. Digital infrastructures with critical mass of users should in addition provide access to third-party providers under fair, transparent and non-subjective conditions.

A European or global identity standard could improve AML compliance in the crypto space by providing customers' KYC information that could help fulfilling mandatory AML requirements.
Considering the impact that programmable digital money can have on business processes and the facilitation of cross-border activities, legal clarity must be provided at the international level. European consumer protection standards must be upheld, based on today's regulatory framework.

Following out of the risk categories highlighted above, the EBF would like to flag relevant aspects on the assumption of a privately issued stablecoin solutions:

- Negative impact on the monetary policy due to reduced central bank influence and, in turn, reduced monetary policy effectiveness. By concentrating monetary power in the hands of a private issuer with international customer base, competition issues have to be considered (see also the G7 report on stablecoins, 2019). A small user base on the other hand is no indication that systemic risk can be excluded. The systemic relevance of a stablecoin – or absence thereof – cannot be definitively concluded at the beginning of the issuance process (in particular looking at a payment service), since their significance for the system can change later on due to extending user base.
- Both retail and business users run a foreign exchange rate risk with the private stablecoin issuer. The risk is determined by the issuer and by privately controlled "events" intruding its decision making.
- Potential regulatory arbitrage due to a missing taxonomy for crypto-assets, including stablecoins.
- Private stablecoin issuers could aim for a close connection of their services with existing electronic identification tools of their members, specifically large social media companies outside of Europe. This triggers privacy concerns. Linking customers' use of the stablecoin to existing identity markers, e.g. online accounts of social media, can produce unprecedented data portfolios. It will be vital to ensure that EU residents' personal data is processed in accordance with EU legal standards, especially when the data is transferred to third countries, in line with the GDPR framework. Because the division of responsibilities between private issuers and wallets is unclear, KYC cannot be guaranteed. This undermines AML activities.
- Technically, there currently is no concrete indications that transacting of a privately run stablecoin network will be permissioned or limited only to identified participants under KYC policies.

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.

Any stablecoin arrangement has the potential to become global. Therefore, it appears not recommendable to distinguishing between 'stablecoins' and 'global stablecoins' per se. Instead, a discussion could distinguish between 'stablecoins' and 'systemically important stablecoins', i.e. those stablecoins that have the propensity to impact global financial stability.

The latter create a higher risk for financial stability. Global private stablecoins could become too-big-to-fail; a potential run on privately issued stablecoins worldwide would create wider repercussions on financial markets in case the private global stablecoin issuer would be forced into fire sales.

A globally successful private stablecoin, issued by a non-bank entity, could undermine bank deposit funding. This is a significant side-effect, which could arise from the use of crypto-assets and should therefore be considered when considering targeted regulation. As one of the main function of banks is to engage in maturity transformation – which is the transformation of short-term liabilities, like deposits, into long-term assets, such as mortgages or SME credit – the ability of banks to exercise some of their core functions would be negatively impacted if deposit funding would see a significant decrease as a result of the increasing use of stablecoins.

In extremis, a privately issued stablecoin with global reach and respective user base may undermine the ability of nation states (depending on geography and market) to define their own money or conduct monetary policy. If a private stablecoin initiatives would establish itself as an alternative means of exchange in transactions to publicly issued currency like the Euro, central banks would be impacted in their ability to carry out their mandate to intervene in the economy of their respective jurisdiction through monetary policy. Consequently, licensing and oversight processes will be an important aspect of supervisory control for initiatives with systemic reach.

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.

The principle “same services, same risks, same rules” should apply when considering a regulatory activity targeting a crypto-assets ecosystem. Under the current market dynamic, non-bank entities emerge, targeting the provisions of financial services (such as payments). Individual initiatives – should they get recognized by authorities in different European jurisdictions – have the potential to gain systemic effects. In turn, they should be subject to the same level of regulatory safeguards as traditional financial institutions.

The questions of a bespoke regime for crypto-assets require a continuous exchange of regulators and stakeholders under careful considerations of implications and value.

On the one hand, legal certainty can contribute to a clear protection of customers, investors and financial industry. A level-playing field at the EU level could provide grounds for European companies to scale-up at EU level, overcoming local discrepancies in different jurisdictions. In turn, the EU’s global position in this evolving economic phenomenon could be enhanced.

On the other hand, a specific regulatory regime for crypto-assets would add to the regulatory burden for the industry. Operating under an – only adjusted – regulatory framework avoids the danger of overall overregulation. Leveraging the existing rules, different categories of crypto-assets (see above Q. 7) can be considered when assessing the applicability of today’s regulatory framework. Any respective discussion should look at:

- security tokens: to be regulated like securities and other financial instruments

- asset-backed stablecoins: to be regulated as the underlying asset (e.g. stablecoins backed by cash could be regulated like e-money);
- native crypto-assets: considered as digital commodities in some jurisdictions, since the market price is determined solely by supply and demand and where the supply may be limited according to some algorithm.

The simple fact of issuing a financial instrument on basis of a new technology (without changing economic function) does not call for a creation and application of new specific rules. Rather, an appropriate amendment can adjust the rules and requirements, accordingly, offering at the same time a chance to acknowledge the benefits of DLT for conduction of business (e.g. transaction recording). Where technological innovation faces barriers due to regulation, a continuous exchange of regulator and stakeholders can help to develop appropriate guidance, recognizing regulatory expectations and aiming for legal certainty for market participants.

This approach would ensure that the regulatory framework remains technology agnostic in order to encourage innovation and foster a level playing field. A principles-based approach would help to mitigate risks and fulfil regulatory objectives while at the same time ensuring flexibility required for a future proof framework.
Crypto-assets are of global relevance due to its digital nature. The EBF supports an exchange at the global level among regulators and stakeholders, aiming for a consistent approach to ensure an appropriate protection for investors and consumers as well as financial stability. Avoid regulatory arbitrage across Europe would help to facilitate the development of innovative financial services in and beyond Europe.

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

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

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

Considering amendments to supervisory and regulatory requirements in different states such as Germany, Italy, Luxembourg, Lichtenstein, France and Switzerland, legal certainty and regulatory clarity receive increasingly attention.
The EBF supports the fundamental principle of “same services, same risks, same rules” when considering an approach to crypto-assets under a regulatory framework.

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.

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

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

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

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

In light of the technological development, a continuous engagement of the Basel Committee with stakeholders is welcome. The close attention that European institutions and regulators in Europe (and beyond) are paying to crypto-assets is appreciated, looking at benefits but also acknowledging the clear risks involved with crypto-assets such as stablecoins (see for example the joint Statement of the European Commission and Council on "stablecoins", 5 December 2019).

Greater clarity regarding the prudential treatment of crypto-assets will help financial institutions to take part of this market. The Basel Committee on Banking Supervision takes steps to engage with stakeholders already. It is important that any effort on this front is coordinated at international level to ensure a level playing field across different countries and jurisdictions.

Moreover, it should be ensured that the prudential treatment of crypto-assets reflects the nature and risks of the different types of crypto-assets, consistent with the principle "same service, same risk, same rules". This implies that for those assets that perform an analogous economic function to other traditional asset classes

(or that are a representation of the latter), the existing prudential treatment for those assets should be applied. This refers to those crypto-assets that qualify as financial instruments under MiFID or as electronic money under the EMD2, but also to those crypto-assets that are a virtual representation of a physical asset (i.e. real estate).

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.

The token economy operates across borders, hence requiring a cross-border international coordination to appropriately address risks involved and avoid fragmentation of the regulatory approach.

As long as a coherent international regulatory framework is amiss, the legal uncertainty around crypto-assets hinders systematic investments by the financial industry. In turn, the development of DLT is slowed down. European banks recommend a technological neutral approach to provide clarity to the market regarding crypto-assets applicable regulatory requirements. Without such clarity, implementation of potentially innovative DLT-based functions will be missing, ultimately to the detriment of consumers, companies and the broader financial system.

Recognizing the variety among crypto-asset products and services – traded through DLT platforms – use cases should be recognized by authorities according to their activities in question. In order to understand the necessary nuances for required guidance, the financial activity, not the technology alone, should determine regulatory actions.

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.

Appropriate harmonization can support legal clarity, ultimately fostering cross-border business within the European market.

A pan-European approach should be discussed, aiming to avoid the divergences that different national legislative initiatives would introduce, and which would hamper the development of services for the whole European market. Fragmentation would limit growth of DLT applications across the EU.

Appropriate clarification regarding legal validity of token transfers and the tokenization of other assets should be considered under an appropriate timeframe. A considerate harmonization of national laws should be addressed before the finalization of the CMU or the removal of other long-standing legal obstacles for securities.

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.

Drawing input from individual European Member States' markets, the following service providers can be indicated as related to crypto-assets:

- Exchanges (fiat-to-crypto-assets);
- Trading platforms;
- Custodial wallet providers;
- Payment gateways for e-commerce.

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.

Regulatory activities should consider the principle “same services, same risks, same rules”. Even if crypto-assets may pose challenges as to the traditional connections between conduction of business and physical location, appropriate investment protection safeguards must be upheld also in the realm of crypto-assets.

In order to create a comparable level of investor protection with security tokens covered under MiFID II, the client categorization could be applied: physical presence in the EU requested for serving retail clients; non-physical presence possible for serving professional and ECP clients according to national legislation. This entity should also comply with all the legislation and the prudential requirements.
Compliance is appropriate regarding the following regulations and requirements: AML / CFT rules, ensuring prudential requirements, consumer and investor protection considerations, applying the same business to same regulation principle, access to the internal market.

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.

As a matter of principle, the issuer of crypto-assets should be responsible for the disclosure. The EBF believes that disclosure in relation to the issuance of crypto assets should take into consideration specific rules regarding investor protection, allowing for a level playing field with issuance of traditional financial instruments under existing legislation (“same service, same risks, same rules”). National competent authorities should be involved in the process of issuance, in order to monitor potential frauds in ICOs of crypto assets.

To this extent, the EBF supports a gradual regulatory approach that would entail the design of specific requirements for the drafting and transparency of white papers accompanying the issuance of new crypto assets. In this respect, while not automatically granting the right to issue crypto-assets (for which an authorization would be needed), white papers encompass less detailed information as opposed to a prospectus but bear the advantage of facilitating SMEs’ access to finance. Such regulatory approach should consider the question of liabilities for disclosure (risk inherent in the crypto-asset/activity in question),

transparency of information requirements – proportionate to the type of asset and related material risk – and regulatory status of the issuer.

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.

Information requirements under legislation and their interaction with crypto-assets require further careful consideration. At this point, understanding of technology and consequences for legislative interaction are an evolving process.

The EBF would like to highlight considerations of European banks that crypto-assets (such as investment tokens) could meet the criteria of legal definitions under national regulation. In turn, regulatory obligations could come into play, requiring a prospectus. In such constellation, the clarification of interaction with European legislation, including information requirements under MiFID II, can be necessary.

Consumers and investors require appropriate transparency and understanding of the asset in question to make informed decisions. Looking at the variety of possible crypto-assets – see Q. 8 – there should be a nuanced consideration of information requirements for investment tokens different from other token

categories. The number and design of information documents for tokens other than investment tokens should be carefully assessed. In order to allow not only for transparency but also understandability, there should be options for simplifying and rationalizing the required information in the latter case.

Looking at potential risk by inadequate advertising rules, misleading promotions or aggressive solicitation (digital communication channels), Directive 2005/29/EC concerning unfair business-to-consumer commercial practices should be assessed for further clarification in terms of crypto-assets.

The principle “same services, same risks, same rules” must apply. European banks believe that all the requirements relating to financial markets – as set out in different pieces of EU legislation – would need to be applied to crypto-assets (not covered as financial instruments by the legislation directly) once they bear the same risk (even sometimes a higher level of risk) than financial instruments. The economic function of the asset shall be considered carefully.

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.

Following the principle ‘same risk, same service, same rules’, the EBF believes that legislative and non-legislative clarification would permit to achieve a higher level of investor protection. If a need for clarification becomes visible, EC and ESMA can operate within their given competences, considering RTS and Q&As if need be.

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.

Following the principle “same services, same risks, same rules”, token used for payments services should be subject to requirements as codified under PSD (e.g. licensing obligation).

On top of the issues mentioned under Q.23, and in order to avoid potential transparency issues as such that the one which took place a few years ago with crowdfunding, we believe that crypto-assets issuers should be subject to a number of minimum requirements, including MiFID investor profile and client categorization as well as cost transparency.

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.

At a larger scale, we support the application of MIFID client categorization and cost transparency to crypto-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.

Though non-objective criteria could be used to make a distinction between different users of crypto-assets and the volumes traded, the EBF does not consider objectives criteria to offer a clear distinction between stablecoins and global stablecoins. Any stablecoin arrangement has the potential to become global. Therefore, it appears not recommendable to distinguishing between 'stablecoins' and 'global stablecoins' per se. Instead, a discussion could distinguish between 'stablecoins' and 'systemically important stablecoins', i.e. those stablecoins that have the propensity to impact global financial stability. Crypto-assets in general can be considered global due to their digital nature. Focus should be on the potential impact of the individual initiative for the financial system or the economy, e.g. due to its potential reach (e.g. when sponsored by large technology or financial firms with a large customer base), the number of assets used for the reserve, the targeted customer market and the volumes involved (e.g. transactions). Furthermore, traditional criteria for systemic status (for instance by the Basel Committee) can be considered for application: size (by number and value of stablecoins in circulation), the degree of interconnectedness with the financial system (i.e. composition and management of the reserve), the degree of substitutability in case of failure, the complexity of the business model and the degree of cross-jurisdictional activity involved. It is to note that some of these criteria could rather apply to the infrastructure in question than to the stablecoin issuer (e.g. complexity).

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			
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.

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

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

A European or global identity standard could improve AML compliance in the crypto space by providing customers’ KYC information that could help fulfilling mandatory AML requirements.
The processing of personal data in connection with programmable digital money requires viable data protection.
Private issuer could aim for a close connection of services with existing electronic identification tools of its members, specifically social media companies with extended user database. Linking customers’ use of the stablecoin to existing online accounts of social media providers can produce unprecedented data portfolios. It will be vital to ensure that EU residents’ personal data is processed in accordance with EU legal standards, even when the data is transferred to third countries, in line with the GDPR framework.

As part of the necessary legal certainty for market participants, clarity is required if transacting on networks of private issuers will be permissioned or limited only to participants after conduction of KYC. As of now, permissionless transacting by private issuers can't be ruled out.

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.

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.

In line with Q. 24, it appears advisable to make the distinction for stablecoins along the line of being “systemically important” or not. Under the previous distinction by stablecoin and “global” stablecoin, most of the requirements under Q.25 appear relevant. However, looking closer at the systematical importance, differences would come into effect. While requirements to segregate and ring-fence customers’ funds should in principle be applicable to all issuers of stablecoins, be them global or not, prudential requirements or requirements to deal with the failure or interruption of operations, and the intensity of oversight and auditing requirements should be proportional to the risks posed by the stablecoin initiative. As such, these should be tighter in the case of systemically important stablecoins.

“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.

Regulation of crypto-assets should follow the underlying principle “same services, same risk, same rules”.

Regulatory treatment will depend mainly on the features and economic function of the asset and, where possible, application existing frameworks. Hence, included distinctions of this framework in terms of customers apply to the crypto-asset. For example, following the logic for consumer/investor protection rules under MiFID II, different levels of protection are appropriate for retail clients, professional clients and ECP. Retail stablecoins would receive a stricter regulatory treatment then wholesale stablecoins.

2. Trading platforms

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

The following extra risks can be identified: lack of liquidity, potential issues of price information and potential remote access for buy-side customers (markets participants purchasing stocks, securities, and other financial products based on the needs and strategy of their company's or client's portfolio needs).

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.

According to European banks, the issues under Q.27 prove to be even more relevant when taking into account the potential over-multiplication of platforms in a DLT-based environment.

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.

Among other requirements that could be imposed on trading platforms in order to mitigate such risks there are: an appropriate governance, appropriate controls and role of the user committee.

28.2 Please indicate if those requirements should be different depending on the type of crypto-assets traded on the platform and explain your reasoning for your answers to question 28:

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

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

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

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

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

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

A lack of transparency can lead to foreign exchange risks: both retail and business users may run an exchange rate risk with private organizations issuing stablecoins (incl. systemically important stablecoins). The risk is determined by the private organization itself and by possible events and key decisions intruding the exchange process.

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.

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

5000 character(s) maximum

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

4. Provision of custodial wallet services for crypto-assets

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

Great risks include consumer protection, fraud and money laundering/terrorist financing. In addition, technical evolution itself can inherit additional risks due to unmitigated grey zones, triggered by regulation slow to adapt to the rapid technological developments. FinTech could be used in ways that were not intended and can cause significant harm. The stringent regulatory and supervisory framework for the financial sector provides incentives to use other types of service providers that are not subject to such obligations or controls. This not only applies to potential fraudsters, but also to common businesses that consider requirements imposed to banks too cumbersome and expensive Other risks worth mentioning are bankruptcy of the counterparty and settlement finality vis a vis irrevocability.

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.

Learning from the experiences of European banks on a continuous basis, risk considerations under Q.31 cannot be considered static but follow the development of technology and business operations by custodial wallet service providers in the different Member States.

As a general principle, the EBF believes that the same regulation that applies to regulated entities that act as custodian of money or financial instruments should apply also to other players when delivering these services. This carries aggravated risks in case of third country counterparties not operating under EU prudential requirements and regulation.

Custodian wallet service providers offer services that resemble to the ones offered by financial institutions. However, unlikely to these providers, financial institutions operate under considerable regulations and are subject to supervision. In the interest of the fundamental principle “same services, same risks, same rules”, the consumer protection level should be able to rely on a level playing field between wallet providers and financial institutions. When dealing with a custodian wallet service, protection should not be lower than the established regulatory and supervisory safeguards for banks.

To store cryptocurrency should be ensured by the same protection level as storing fiat currency in a bank.

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

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

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

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

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

Audit and compliance functions should be considered.

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.

Crypto-assets classifying as financial instruments should be considered as such under MiFID II. Hence, securities market regime and rules of conduct with regard to their custody and management and the rules for the protection of clients' assets should apply with the proper adjustments.

When virtual assets cannot be considered financial instruments, in order to guarantee consumer protection (e.g. in case of insolvency of the custodian or in case of loss of crypto assets), a specific regime could be established for the authorization, operation and supervision of custodian entities that includes the particularities of the custody of crypto-assets. The latter may be based on the principles set out in the securities market conduct of business rules on custody, in a manner that is proportionate to the risks.

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

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

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

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

Custodial wallet providers should meet the same requirements as any other custodian of money or financial instruments (same service, same risks, same rules). Custody and safekeeping of tokens, including the tokens qualifying as financial instruments, are of great importance. Regulatory requirements should be applied (depending on the legal nature of the asset), ensuring the appropriate level of safekeeping.

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.

Gateway services accepting payments for e-commerce should be considered, as well as all services and functionalities under smart contracts.

There should be no intentional distinction between homologous digital wallets and crypto-asset related wallet services. Applicable principles should cover acquiring of services (merchant POS), onboarding and payments.

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.

In the perception of European banks, asset valuation procedures including ESG and climate risk factors should be taken into consideration as requirements, in order to properly align with non-financial reporting directive and the EU taxonomy.

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.

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.

European banks support the establishment of regulation on a technology neutral basis. Therefore, if crypto-assets are used for making payments, they should be subject to the EU payments legislation, regardless of the underlying technology ("same services, same risks, same rules"). This allows for a level-playing field as well as appropriate risk mitigation.

Rather than new regulation specifically on the use of crypto-assets for the purpose of payment transactions, a more specific classification could help to establish (ex ante) how any given process for something in the general vicinity of payments is to be classified, and hence to be regulated under existing regulation for payments. Banks recognize that stablecoins can be used for making payment transactions as well. We believe that these products, if used for payment transactions should face the same scrutiny as any other payment product when it comes to security and customer protection as stipulated in PSD2, data privacy as stipulated in the GDPR as well as requirements related to AML, KYC, ATF and other legal requirements. A level playing field should exists between all payment products.

Generally, we remain open to related developments in the area of stablecoins/digital currencies and their potential use for payment transactions. We think however that further research is needed before being in a position to draw definitive conclusion. We note that in some discussions, it has been stated that a global stablecoin could be needed in order to facilitate cross-border payments. In the European context we do not

see such a need, as cross-border payments are already well developed and regulated, and instant cross-border payments are already a reality, to expand shortly.

The digitalization of the economy and today's daily life places new demands on digital forms of money. Programmable digital money, whether account-based or token-based, could be a key element of the digital transformation and play a major role particularly in connection with smart contracts. In this area, Europe must keep up with this competition so that the global financial architecture does not lead to a polarization between solutions originated in other areas of the world. Any initiative on central-bank issued digital currency should include the banking industry and should not seek to replace private sector actors but should target a common exchange between the European System of Central Banks and European banks.

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.

As far as market functioning is concerned, market integrity should be ensured in order to prevent systemic and propagation risks. In particular, measures should be undertaken in order to prevent short-selling practices by focusing on the correct provision of market transparency and price formation. Specifically, the regulatory regime of DLT-based assets trading should safeguard investors against any manipulation of the underlying asset.

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.

Trading of DLT-based instruments and tokenized assets increases the exposure of investors to propagation risks and market conduct issues, the handling of which will be essential to safeguard investors' interests and ensure a fair and orderly market for tokenized assets. Recourse and redress in case of damage due to a technical issue, theft or non-existent real asset backing the tokenization is only some examples of such investor risk involved.

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.

It is our belief that all crypto-ecosystem participants (such as advisors, incubators, miners, developers, sponsors, etc.) should necessarily be subject to the same regulatory regime developed for and applied to a classical financial ecosystem (i.e. setting up rules, full supervision and sanctions), following the principle "same services, same risks, same rules". The underlying economic function of the crypto-assets is essential for determining the regulatory approach.

In this, the EBF supports IOSCO's view according to which fostering innovation should be balanced with the appropriate level of regulatory oversight. In line with OECD conclusions in its January 2020 report and the thinking of the Joint Statement of Commission and Council from 5 December 2019, EBF members believe

tokenized markets should comply with regulatory requirements that promote financial consumer and investor protection, market integrity and competition and seek to guard against build-up of systemic risks.

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.

The EBF believes that the most effective way to ensure an adequate level of market integrity and investor protection is to establish an appropriate regulatory regime as clearly as possible. This includes effective market supervision, an authorization process and reporting requirements to the NCAs to ensure proper supervision.

39.1 Please explain your reasoning for your answer to question 39:

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

In line with our response to question 38, it is our belief that, all crypto-ecosystem participants (such as advisors, incubators, miners, developers, sponsors, etc.) should necessarily be subject to the same regulatory regime developed for and applied to a classical financial ecosystem (i.e. setting up rules, full supervision and sanctions), following the principle "same services, same risks, same rules".

In this, the EBF supports IOSCO's view according to which fostering innovation should be balanced with the appropriate level of regulatory oversight. In line with OECD conclusions in its January 2020 report and the thinking of the Joint Statement of Commission and Council from 5 December 2019, EBF members believe tokenized markets should comply with regulatory requirements that promote financial consumer and investor protection, market integrity and competition and seek to guard against build-up of systemic risks.

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.

EBF members agree on the principle that any platform trading EU crypto-assets or trading in the EU should fall within the remit of EU rules and EU supervision in order to ensure protection of EU investors.

As crypto-assets have the specificity to be distributed cross border, we believe supervision should be ensured at EU level to aim for a higher degree of effectiveness. Supervisory collaboration with competent authorities in third countries will be a helpful step to prevent circumvention of requirements.

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.

European banks consider it important for crypto-assets to operate under a consistent regulatory framework across Member States' jurisdictions.

There is merit in the alignment of the EU AML/CFT legal framework with the broader definition of crypto-

assets provided by FATF. In our view, this definition is more appropriate to reflect the relevant potential development of crypto-assets for investment purposes, also due to the digitalization of the banking sector and the related increasingly presence of FinTech companies. In addition, EU definitions should be aligned with a common global crypto-asset taxonomy, creating a common understanding of terms.

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.

Depending on their nature and respective definition under existing legislation, crypto-assets can be used for the same purposes as financial assets: to make payments, to transfer value, to store value and to increase value. In turn, the possession or property of crypto-assets can also potentially derive from criminal activity (i. e. fraud). Fraudulently acquired crypto-assets could be converted in other crypto-assets.

Hence, crypto-assets are open to the same use for ML/TF as financial assets. To not include crypto-assets in the EU AML/CTF legal framework would provide more incentives to criminals to increase the use of such assets, thus making ML/TF harder to detect and to investigate. More specifically, covering only one moment of the exchange (fiat-to-crypto) would make it impossible to detect many illicit transfers. The same considerations could be applied to payment gateway providers.

Finally, some national regulations extend the AML/CFT legal framework to every crypto-asset service provider. It is therefore important to maintain a level playing field across the European Union, adding crypto-asset services to the AML/CFT legal framework obligations.

In addition, a clear definition of "security token" and "utility token" and the related market regulation should be given (i.e. the access of the market for a crypto-asset service provider and the access of the services offered by this provider to investors) in order to clarify risk services as ICO (Initial Coin Offerings).

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.

The technical evolution is very fast and legal frameworks and regulations face the challenge to adapt. In line with the “same services, same risks, same rules” principle, the actual requirements for technology platforms should be the same as financial institutions, to the extent they provide the same services. Crypto-assets allow customers to make payments, transfer value, store value and increase value in a new way, but there is still a case of the same functions performed by regulated financial institutions. Same functions and same risk should be met with the same rules.

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.

In the current ecosystem of cross-border and digital transactions, the EBF acknowledges the need for establishing the appropriate measures to mitigate the ML/TF risks associated with crypto-asset activities. In order to ensure a consistent protection against money laundering, there cannot be an unjustified differentiation between traditional financial institutions and other market participants. As a general remark, it is important that the same regulatory standards apply to all actors facilitating the transfer of value/funds through financial services, regardless of whether they are made through financial instruments, fiat currencies, traditional or crypto solutions, on the basis of the principle “same services, same risks, same rules”.

Financial institutions are being highly regulated and know-your-customer (KYC) checks are an essential process in their anti-money laundering efforts. On the other side, criminal networks show an increasing sophistication in identifying and targeting the weakest link in the value chain. In case crypto-asset service providers would be excluded from the status of ‘obliged entities’ under EU AML/CFT framework, the resulting lack of requirements would leave room for weaker defences. In turn, criminal networks could exploit this lower level of protection, ultimately undermining the AML efforts by financial institutions. Ensuring that crypto assets service providers comply with the same rules as financial institutions would make it easier for the latter to engage in doing business with such providers, if able to deliver KYC information.

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.

Peer-to-peer transactions without intermediation of a regulated service provider prove to be vulnerable to money laundering due to the absence of monitoring tools for this relationship.

Future regulatory work should reflect the new, specific and increased ML/TF risks arising from peer-to-peer transactions. Policy-makers shall ensure that the build-up of an effective legal framework allows financial institutions that provide banking services to crypto-asset service providers or to customers involved in crypto-assets activities to apply sound know-your customer/ enhanced due diligence (KYC/ EDD) procedures and an effective risk-based approach to those new players. This should include consideration of transparency in transaction chains involving the virtual assets and how far technological and market developments support this, for example, the availability and cost of effective blockchain analysis tools and how far these techniques are undermined by developments in privacy coins, tumblers and other relevant crypto asset service providers' products and services. Moreover, in order to avoid anonymous transactions or transactions performed by sanctioned individuals, it should be mandatory for crypto-asset service providers that the relevant AML/CFT data/information (i.e. Identification data, copy of IDs, source of funds and scope of the transactions) are hold by crypto-asset service providers and make it available upon request to competent authorities in compliance with EU record keeping requirements.

Effective regulatory action should ensure that banks do not solely assume the costs and risks associated with the entrance of those new players. Without tailored rules to be applied and enforced vis-a-vis crypto asset service providers, financial institutions will find it very challenging to assess and manage the ML/TF risks of crypto-asset service providers and compliance with their AML/CTF responsibilities will require an increasingly number of such business relationships to be declined or closed. In this case, ML/TF threats could be transferred to non-financial sectors or to non-regulated environments and channels, increasing the related risks in Europe.

European policymakers should ensure that, together with legislative action and regulatory work on this field, Financial Intelligence Units (FIUs), the European Supervisory Authorities and National Competent Authorities shall play a leading role promoting the knowledge, expertise, training and information sharing with banks, as well as the use of new IT solutions that might assist banks and other obliged entities in effectively understanding and handling the ML/TF risk factors raised by crypto assets/ crypto asset service providers. European policymakers should also show leadership in supporting accelerated implementation of FATF standards across Europe and support FATF and other international bodies in establishing a consistent global framework.

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.

In alignment with the EU AML/CFT framework and from an AML/CFT perspective, it is important to ensure coherent and detailed actions for risk mitigation towards new and risky financial actors, in order to avoid potential criminal actions in a grey legal framework. Regulation of crypto-assets/ crypto-asset service providers shall comprise the adoption and effective implementation of a resilient European supervisory framework, ensuring that the specific ML/TF risks involved are effectively identified, addressed and mitigated, by the EU institutions, the European Supervisory Authorities, National Competent Authorities and Financial Intelligence Units (FIUs), so as to avoid imposing additional compliance burdens to banks regarding new players that carry new risks and requesting banks to prevent the negative effects for the financial system as a whole that derive from a potentially “free riding” behaviour.
Effective capacity of public institutions and all the relevant AML/CTF stakeholders is needed to progressively identify, understand and deal with the idiosyncrasies of crypto-assets and with the specific structural elements of crypto-asset service providers channels in a proactive way.

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.

On the basis of the principle “same services, same risk, same rules” providers of services related to crypto-assets should be covered by similar regulation than financial institutions. This would lower the risk of such providers to be under the potential control of criminal actors. It would be important as regards the providers’ relationship with their business partners, such as financial institutions, and help them secure necessary financial services, such as bank accounts.

For further guidance on the design of a fit and proper test for directors and senior management of crypto asset service providers, the European Central Bank’s guide to a fit and proper assessment could be considered.
Lastly, the opportunity to set up the new function of crypto-asset officer (both on client side and own account side) may be taken into consideration. In parallel with the AML officer, such professional figure may be responsible for regulatory implementation at an institutional level. A crypto-asset officer’s primary professional focus would fall on the internal control systems that the institution puts in place to help detect, monitor and report unsound activities to the authorities.

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.

We believe that priority should be given to guarantee consumer and investor protection against the risks inherent to crypto-assets through a technology-neutral approach.
Information provided to consumers, before, during and after the conclusion of the financial contract, represents a crucial aspect in terms of consumer protection.

In this context, the quality, clearness and simplicity of the information delivered to customers are key aspects of the provision of information on financial contracts which enables investors to make more informed decision. On the contrary, it has been proven that long, detailed and rigid list of information on the financial agreement overload consumers with unnecessary details that might switch off their attention or retract their willingness to invest.
For these reasons, the EBF believes that clear, simple, future-proof and overarching rules concerning the provision of information on crypto-assets are essential in order to guarantee consumer protection, and to embrace the digitalization of the financial market. More specifically, the timing of the EU decision-making process in terms of negotiations and implementation makes continuous adjustment of the legislation in response to the changes in technology evolutions of the digital market very difficult. Therefore, ensuring that legislation is principle-based and technologically neutral is necessary to allow it remaining relevant to subsequent and potentially rapid technological changes.

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.

Looking at the proposal under Q. 47 for limits on the investable amounts in crypto-assets, one should consider that limit requirements for provision of services related to investment products are based on specific features of security asset-classes (equity, bon, derivates, units in collective investment undertakings etc.). Investment tokens cannot be considered a specific asset class under financial instruments. Consequently, the idea of limits would require precise reconciliation of crypto-assets with asset-classes of financial instrument. Should token classes not serve investment purposes, an extended requirement from the realm of investor protection should be carefully evaluated in terms of its possibly excessive nature.

The EBF welcomes a continuous exchange with the regulator based on classes outlined in Q.8.

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.

Underlying the principle of "same services, same risks, same rules" is the central understanding of a risk-based approach. Considering the different crypto-asset types – see Q. 8 – different risk potential of crypto-assets must be acknowledged. For example, utility tokens should not be treated the same as cryptocurrencies. The prevalent economic or social function can determine the seriousness of risks connected to the asset.

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

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

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

49.1 Please explain your reasoning for your answer to question 49:

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

Building on the understanding of the regulatory framework, e.g. MiFID II, different standards are acceptable for classifications of clients: retail, professional, eligible counterparties.
Since private sales appear to be directed often at institutional investors, the nature of private or public sale can allow to target client classifications. Lighter standards for private sales could be the consequence.

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.

Considering the payment commitment and related expectations, a more effective protection for obtainment of crypto-assets (as non-financial instrument) against payments seems favorable. Such standards should also ensure liquidity by safeguarding the possibility to sell at any time against payment.

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.

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.

The intrinsically cross-border nature of crypto markets and crypto players suggests that rules will be most adequate when they are installed at a sufficiently international level.

A coordinated approach to crypto-assets by the European Commission, international bodies and third country authorities can help to address diverging requirements in order to ensure a progressing protection of consumers and investors.

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.

Following the principle “same services, same risks, same rules”, supervision of all crypto-asset service providers should be conducted by the established competent authorities, having investor protection as a core part of their mandate and following the same considerations as for traditional assets, addressing the same issues and risks consistently.

Question 53. Which are the tools that EU regulators would need to adequately supervise the crypto-asset service providers and their underlying technologies?

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

The following considerations are commendable for creation of a framework to enact supervision of crypto-asset services:

- The application of appropriate prudential requirements, including capital requirements, can help to ensure the stability and the solvency of service providers.
- To safeguard important transparency, mandatory disclosure requirements can be considered.
- Governance arrangements need to be ensured, especially on ICT security.
- Appropriate records of users' transactions are needed to limit fraud or potential money laundering operations.
- Embedded supervision, a regulatory framework that provides for compliance in tokenized markets to be automatically monitored by reading the market's ledger, thus reducing the need for firms to actively collect, verify and deliver dates.

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.

EBF members pointed out the following recent regulatory developments in Member States:
- In France, a law on the issuance of DLT-based tokens and on the certification of custodians has entered into force
- A crypto-asset regulation in Luxembourg
- In Germany, the possibility to issue licenses for crypto-asset custodians
- In Italy, Consob (securities markets authority) published the final report on ICOs and crypto-activity exchanges, drawn up after a public consultation on the initial offerings, with a view to the possible definition of a regulatory regime at national level governing the conduct of public offers of crypto-activity and related negotiations
- In the Netherlands, the Dutch Central Bank proposed a dedicated national licensing system

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

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.

Technological development in the field of DLT is continuously ongoing, adding to the potential of efficiency for IT processes. In turn, a finite statement under Q.55 remains challenging, since it depends on technological evolution over time. However, the EBF recognizes the potential.

Transaction’s reconciliation is one of the critical operations in every financial institution and the effective management of this activity is essential to the success of an organization. The main objective of performing reconciliation is to identify incompatibilities in data and achieve resolution.
Reconciliation is an important function in the areas of cash management, payment processing, GL accounting, pre- and post- trade settlement, position management, confirmations and risk and compliance management. While this process is usually time-consuming, a DLT-based mechanism would allow market participants to rely on a unique record to which each party can have access. This would in turn allow a better traceability of records and shorten the duration of clearing procedures.
However, this should be enabled while making sure that distributed ledgers do not overburden standard operational procedures by disallowing the vigilance of human operators along the settlement and clearing

chains.
Other relevant advantages of DLT technology can be expected in the areas of standardization and interoperability.

When compared to the legacy system, financial transactions reconciliation in the post-trade markets represents a potential area where the use of DLTs is likely to generate positive spillovers. All providers of post-trade services carry out regular audits of their IT systems to further improve the functioning of all processes. Regular and timely reconciliation procedures help detect problems almost instantaneously.

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.

Although the EBF is in favor of a market-neutral approach, we acknowledge that the application of permissionless DLT for the trading and post-trading of financial instruments is likely to also pose risks and imbalances for retail and institutional investors and buyers. For instance, in order to be effective, a new DLT-based architecture should take into account a new definition and arrangement of roles and functions of post-trade actors. While respecting a market-based logic, it is necessary to make sure that regulation does not come at the expense of risk when applied to disruptive innovative technologies.

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.

The EBF believes that the adoption of DLTs will not only impact the role and operation of trading venues and post-trade financial infrastructures, but it will also create many opportunities in the medium-long term.
We do not expect that relevant business-changing developments will significantly disrupt the post-trading market in the next 5 – 10 years. We do, however, retain this to be more likely to happen on 20 years stretch.

Considering the impact of such transition in the next years, we believe that a transitional phase in the post-trading business should be introduced to test the emergence of new DLT-based trading practices impacting market venues and infrastructures.

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.

Legal certainty can help market participants to leverage the innovative potential of technology. However, the regulatory development should not ignore the evolution of solutions in the realm of permissionless ledgers, but rather allow for incorporation of innovative technological solutions to the benefit of customers and institutions. The EBF invites regulators and stakeholders to continuously engage in respective discussions, aiming for an appropriate and legally clear approach, balancing innovation and regulatory safeguards. A gradual regulatory approach could act as a positive enabler of fair competition and market practice. In our view, a disruptive regulatory stance would negatively impact the implementation of innovative technological solutions for post-trade services.
An example of this gradual approach could be the suggestion of a regulatory framework of experimentation, aiming for an increased level of innovation which bolsters the EU's competitiveness with other markets.

B. Assessment of legislation applying to 'security tokens'

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

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

1.1 Financial instruments

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

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

In its Advice, ESMA indicated that in transposing MiFID into their national laws, the Member States have defined specific categories of financial instruments differently (i.e. some employ a restrictive list to define transferable securities, others use broader interpretations). As a result, while assessing the legal classification of a security token on a case by case basis, Member States might reach diverging conclusions. This might create further challenges to adopting a common regulatory and supervisory approach to security tokens in the EU.

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

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

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

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

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

A clear understanding and classification of different crypto-asset categories is required to enable proper regulation and supervision according to the assets' characteristics and risks. It is important to consider the underlying economic function of the crypto-asset, allowing for the appropriate application of the principle "same services, same risks, same rules". If characteristics of a digital token are those of a security (i.e. security token), respective regulation should apply. If, on the other hand, characteristics equal those of another financial instrument (e.g. a loan), the latter's regulation must apply. In any case, regulations should be open to be quickly integrated when new categories of crypto-assets will arise.

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.

The EBF appreciates the European Commission's considerations of remedies under Q.60. It will be helpful to establish a continuing dialogue to understand the efficiency of the proposed measures.

As an initial comment, the broad and extensive nature of "transferable security" definition (article 4 n. 44) of MiFID II) introduces legal uncertainty for cross-border business. If not amended, this definition will continue to be subject to different interpretation and application by NCAs. The provision of interpretative guidelines could be a useful solution at a high level.

A clear understanding of security tokens will be useful. However, operating on basis of the existing regulatory definition, the objective should be to determine if a token is a "financial instrument", without creating legal uncertainty as to a potential diverging term of a "security token". All securities are financial instruments but not all financial instruments are securities. If a digital token has the characteristics of a security (i.e. a security token) then it should be regulated as a security. On the other hand, if a digital token has the characteristics of another financial instrument (e.g. a loan) then it should be regulated as such.

60.2 Please explain your reasoning for your answer to question 60:

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

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

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

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

EBF members believe that, in hybrid cases where tokens incorporate combined and different investment profiles, regulators should ensure that end investors are properly aware of the risk of losing their initial investment.

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.

The EBF appreciates the European Commission's considerations for dealing with hybrid cases under Q.61. Considering the evolving technological and business solutions, it will be helpful to establish a continuing dialogue to understand on how regulators should address hybrid cases. Appropriate guidance, learning from assessments on a case-by-case basis, could help to provide orientation to market participants, guaranteeing a level playing field among involved entities in Europe.

This dialogue should address the observation that in cases where tokens integrate different investment-type features, the risk of losing the underlying asset grows as the investment lies exposed to the unintended consequences generated by the increased complexities.

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.

The understanding of necessary requirements for investment firms in a DLT environment is continuously developing. New and additional services and responsibilities for investment firms might arise. Management of investor protection requirements could be located off-chain under the vision of some market participants. This would exclude such management from a direct DLT impact. At the same time, participants refer to the lack of a precise common taxonomy for DLT and the resulting instruments. Should requirements in a DLT environment depend on procedural changes in the provision of investment services, organizations and institutions would be faced with challenging organizational issues. Ultimately, the application of rules and requirements for investment firms in a DLT environment requires further exchanges of stakeholders and regulators to understand the implications, not least on investor protection.

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.

The current regulatory framework is largely based on centralized schemes and responsibilities (i.e. CSDs, CCPs) and is not written with tokens in mind. The provision of guidance on applicability of such rules would be crucial in order to facilitate the access of current investment firms and new actors on the security-token market. Given the innovative nature of the technology used, a useful means in order to evolve the current framework and to accommodate crypto-assets could be a consideration of a regulatory framework of experimentation, aiming for an increased level of innovation which bolsters the EU’s competitiveness with other markets. Particularly, aspects relating to investor education (new services and new obligations must be explained) and rules of transparency (pricing, legal aspect, protection – updating applicable general conditions) must be taken into consideration.

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.

EBF members believe that the current scope of investment services and activities under MiFID II is substantially relevant and should be applied with regards to main services in trading of security tokens. However, they consider that MiFID II, including the MiFID questionnaire, should also apply to ancillary services. Hence a potential revision is to be envisaged to encompass these new instruments.

Question 65. Do you consider that the transposition of MiFID II into national laws or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT for investment services and activities? Please explain your reasoning.

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

Considering that MIFID II is technology neutral towards DLT technology, it should apply to all entities that provide or intend to provide investment services, regardless of the use of this technology. However, the transposition of MiFID II would impair the use of DLT as, MIFID is a heavy regulation which requires IT developments to ensure compliance with its requirements. Thus, European banks stress the necessity to make sure that the use of DLT is safe and to the benefit of investors with a single EU-wide MIFID2 application to securities and security tokens. We believe developing DLT should be made in a safe well-defined and standardized regulatory framework, in order to constitute a viable technical alternative to traditional financial markets. In this, national discretions would make it more difficult for financial institutions to scale and offer services across Europe. The purpose is not to prevent the use of crypto-assets but to make it safer.

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.

In the context of trading venues, EBF is in favor of the application of the definitions and requirements related to their operation and authorization and we don't see any particular issue when doing so. Broadly, EBF members support the setting of requirements as provided by MiFID II regarding conflict of interest, access to

trading platform, trade and price transparency as well as transaction reporting rules to be applied in crypto trading to ensure the proper levels of investor protection.

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.

The EBF supports the application of suitability rules to security tokens. Security tokens are investment products (though not all investment tokens are automatically security tokens)
and clients should be aware of the risks (such as liquidity and capital loss risk) and they should be protected (i.e. through conflict of interest disclosure, costs and trading venues transparency, etc.).

To this end, especially considering the greater liquidity of these instruments, European banks deem suitable the adoption of a preliminary information document related to the offer (i.e. a whitepaper) and/or a documentation associated to the offer, illustrating the investment-associated risks, the related costs, the characteristics of the operation (token utility, resources, returns, etc.), and the exchange platforms where the crypto-assets will be traded.

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.

Looking at the security token class laid out in Q.8, the same requirements apply for social media or online marketing for security token as for any other investment products. Thus, EBF members do not see any merit for additional requirements besides compliance with the principles provided by the current legislation (i.e. Consumer Rights Directive, E-Commerce Directive, EU Distance Marketing of Consumer Financial Services Directive).

Question 69. Would you see any particular issue (legal, operational,) in applying MiFID investor protection requirements to security tokens? Please explain your reasoning.

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

The EBF agrees on the principle that the same rules ensuring the same level of investor protection should apply. As mentioned in Q. 66, security tokens should follow the existing applicable regulation.

However, as far as the process of knowledge assessment under MiFID is concerned, we believe that the way the questionnaire has been designed can lead to significant deadlocks and prevent the proper development of a security tokens investment market as investors are not going to be able to demonstrate that they have a minimum level of knowledge and experience with crypto-asset. Indeed, the whole point of this questionnaire is to demonstrate the appropriate experience to access trading.
With this in mind, although EBF members deem it suitable not to introduce an excessive burden that may discourage the use of these new forms of investment, we believe that innovation should not come as to the expense of risk for investors. For this reason, we believe that a careful evaluation of this phenomenon is necessary in order to ensure the correct balance between innovation and investor protection.

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.

Trading on DLT networks would lower the quality standards that banks and other financial institutions bring to the table.

For SMEs, it is necessary to understand how SMEs can be still considered as such depending on who owns the assets they issue – similar to VC ownership up to X% takes away their SME status even if they have less than 250 employees and low turnover.

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.

In line with OECD conclusions in its January 2020 report, EBF members believe that tokenized markets should comply with regulatory requirements that promote financial consumer and investor protection, market integrity and competition and seek to guard against build-up of systemic risks.
In this regard, the EBF welcomes the application of the corresponding MiFID rules and requirements to DLT-based trading platforms.

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.

EBF members agree that the issuance of crypto-assets should be regulated (Security tokens falling under the definition of financial instruments, see Q.7 and Q.8) and admission to trading should be part of the requirements set up by the authorized trading venue. Specifically, EBF members believe that setting up trading rules will ensure fair, orderly and efficient trading.

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.

Based on the principle of technological neutrality, the fact that a Regulated Market (RM) or a Multilateral Trading Facility (MTF) uses distributed ledger technology should not be grounds to relax the regulatory criteria for direct participation.
The EBF welcomes this position, as a functioning regulatory framework of financial intermediaries not only ensures an adequate level of investor protection while preserving and encouraging access to trading, but it also provides regulatory avenues against systemic risks and for financial stability reasons.

Therefore, a wait-and-see approach based on the principle of technological neutrality is probably best taken in this constellation to follow innovative market developments whilst monitoring at all times broader access to trading venues. As the market can benefit from improved liquidity, permissionless DLT should not come at the expense of investor protection and fit-for-purpose regulations of financial markets intermediaries.

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.

The EBF appreciates a continuing exchange of regulators and stakeholders on the appropriateness of pre- and post-transparency requirements in light of security tokens. There is a need to carefully assess the application and suitability.

A minimum level of pre- and post-transparency requirements regarding price transparency as well as transaction reporting rules could be applied to security tokens, which should on first-basis regulated as other securities. However, European banks also point out that pre-trade and post-trade transparency requirements are based on specific and detailed definitions of specific asset classes. Consequently, this calls for further clarification to make sure that the relevant legislation takes into account any new asset class, thus making transparency truly comprehensive.
The EBF favors trading prices to be provided by data providers to ensure that a high level of market transparency and that prices are widely available to market participants.

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.

The current stage of activities and therefore market data (as well as the precise definition of DLT-based specific asset classes) are too scarce to make more detailed recommendations.

European banks will be monitoring future developments following an increase in trading volumes. In any case, the same minimum rules should apply as based on the principle of technological neutrality.

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.

In the context of proper regulation of DLT-based trading and security tokens trading, EBF members agree that both transparency reporting and the legal obligation to maintain records are of paramount importance. Therefore, their application should be encouraged in order to ensure an adequate level of investor protection and the integrity of tokenized markets. As already mentioned, the same requirements should apply to both security tokens and securities.

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.

The EBF considers the current scope of Article 8 MAR generally appropriate to cover all insider dealing cases. At least, when assuming that all the new market participants determined by the emergence of a new crypto-based financial ecosystem can also be traced back to it. On this, please refer also to the answer to question number 38.

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.

Following question 77, EBF members would agree that as long as Article 12 of MAR makes sure to cover the new market players operating in the crypto-based financial ecosystem, it can be considerate adequate to regulate potential instances of market manipulation.

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.

Following the answer to question 37.1, the greatest risk of unfair market practices in crypto-asset trading takes the form of manipulation of the assets underlying the tokenized securities. This would happen in the case where there are derivatives (i.e. security tokens) whose value is based on an underlying crypto asset (e. g. bitcoin).

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.

EBF members agree on the importance of investor protection objectives in the context of designing the crypto-assets regulatory framework. In particular, given the growing popularity of security tokens among retail investors, the EBF envisages the need to improve transparency reporting on short positions.

80.2 Please explain your reasoning for your answer to question 80:

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

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

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 discriminating factor remains the logic of applying the Prospectus Regulation to the trading of security tokens. Should it be considered appropriate that the security tokens fall within the remit of the Prospectus Regulation, then the same rules should be applied unabridged and without exemptions. If crypto issuance doesn’t fall under the remit of prospectus than a specific regime should be envisaged. For example, a specific prospectus template for security-tokens should be used which could perform the same functionality of a white paper. The specific template should be simplified, considering ICOs and STOs are mainly used by start-ups and businesses in early stages, for which the cost saving is crucial, but the exemptions should be the same. The framework should be technology neutral.

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.

EBF members agree on a full prospectus approach. In particular, in the context of the adoption of new prospectus schedules, our federation's invitation would be to consider including information regarding ESG factors and climate transition. However, should a lighter approach be favored (whitepaper), the same consideration should apply.

The adoption of new prospectus schedules serves to promote transparency and efficiency in the transmission of relevant information to potential investors. In particular, the full prospectus approach aims to ensure that potential investors understand the relevant regulation, risks and specificity of security tokens.

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.

ISIN numbers are granted to financial instruments only. Hence, it would appear that there could be a legal issue, would security token not be defined as financial instrument. Another option could be to assign crypto-assets an "ISIN LIKE" code as it is already the case for certificate and coupons. In case of need, a change in the ISIN standard should be approved in order to accommodate such instruments, e.g. to assign cryptos an "ISIN LIKE" code as it is already the case for certificate and coupons.

Another option is that the smart contract address of the security token (being financial instruments according to Q.7 and Q.8) becomes its ISIN equivalent. The National Numbering Agencies (NNA's) could be required to issue ISIN's for security tokens and other financial instruments. This is not currently the case and presents a barrier to adoption, listing and secondary market trading of tokenized securities.

Question 85. Have you identified any difficulties in applying special types of prospectuses or related documents (i.e. simplified prospectus for secondary issuances, the EU Growth prospectus, the base prospectus for non-equity securities, the universal registration document) to security tokens that would require amending these types of prospectuses or related documents? Please explain your reasoning.

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

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

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

86.1 Please explain your reasoning for your answer to question 86:

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

STOs could provide a useful alternative funding source for start-ups and innovative undertakings whose interests is to avoid complexity and excessive costs. The provision of an alleviated prospectus might therefore be relevant, given the reason behind the choice of raising capital through STOs.

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

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

87.1 Please explain your reasoning for your answer to question 87:

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

EBF members agree on the need to update the ESMA guidelines on risk factors, in particular with a view to ensure consistency between the different national regulatory regimes.

However, in today's capital markets, the risks linked to the infrastructure on which instruments are traded /settled are not required to be disclosed by the issuer. Based on the principles of "technology neutrality" and

"same services, same risks, same rules", the issuer should remain agnostic to those risks when securities tokens are issued in a DLT.

It may be the role of specific entities such as FMIs to take on the infrastructural risks linked to the DLT. This would also reaffirm the safety buffer role played by permissioned trading venues.

The EBF is in favor of maintaining a correct and up-to-date disclosure of the risk factors related to the use of DLTs. Particularly, to ensure a fair and orderly market for tokenized assets, strong efforts should be made to safeguard an adequate level playing field, as well as to implement proper supervisory convergence and investor protection schemes.

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.

Adopting DLT-based solutions could bring about additional opportunities for CSD to provide services. The CSDs already provide necessary notary function and act as a relay for corporate actions and general meeting to all market participants.

Considering that entire range of CSDR legal requirements aim to ensure market stability, reduce systemic risk and promote safety and efficiency in the capital markets, DLT can serve as the underlying technology for securities settlement, provided that it is a private, permissioned DLT system with a centralized validation model.
However, not all types of DLT systems are suitable for mitigating capital market risks: for instance, public permissionless blockchains with a PoW consensus model cannot offer settlement finality, which could impact the stability of the financial system. Such type of DLT should therefore not be considered as fit for purpose.

That being said, regulators may want to clarify how some of the CSDR provisions/notions (e.g. the notion of "account", "book-entry system") have to be applied in a DLT context, so as to ensure that the legal objectives

are met irrespective of the specific technology used.

To this end, regulatory frameworks for experimentation could also be a useful tool to further explore such issues and identify possible gaps.

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.

Please see answer to Q. 88.1.

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.

The EBF believes that CSDR book-entry requirements are compatible with security tokens.

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.

The securities industry carries a significant degree of fragmentation in Europe. Without the proper harmonization between markets at the European level, some countries will continue developing more favorable conditions for the emergence of crypto-assets, while others will lag behind, with the result that there will be high regulatory misalignment and competition issues.

To avoid the risk of fragmentation and distortions also among investor protection regimes and to ensure a robust level playing field, future regulations at the EU level should aim at ensuring a sufficient market harmonization for crypto asset and DLT-related trading.

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.

Please consider the answer to Q. 91.1.

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.

Please consider the answer to question 90.

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.

The EBF believes that security tokens largely fall within the scope of the settlement finality directive. SFD is technology neutral. The definition of a "system" does not refer to a specific technology and allows for a securities settlement system/payment system to be DLT-based. This being said, for the sake of legal certainty and in order to foster innovation and the use of DLT for the settlement of securities transactions, it

is desirable to obtain guidance/clarification from the competent European regulator(s) on how certain notions have to be applied in a DLT context (e.g. notion of “register”, “settlement account” and “collateral security”).

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.

Please consider the answer to Q. 93.1.

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.

According to European banks, SFD rules applying to DLT-based trading and post-trading markets should be clarified as much as possible in order to avoid potential conflicts of laws and increased risks for savers and investors.

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

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

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

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

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.

The answer depends on the way one considers the crypto-asset. Generally, European banks don't yet see any legal issue if the crypto-asset is based on a security token and if – over all – the financial collateral arrangement can be evidenced in writing or in a legally equivalent manner.

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.

Please consider the answer to Q. 97.1

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.

According to Article 9 of the FCD, "Any question with respect to any of the matters specified in paragraph 2 arising in relation to book entry securities collateral shall be governed by the law of the country in which the relevant account is maintained".

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.

According to Article 9 of the FCD, “Any question with respect to any of the matters specified in paragraph 2 arising in relation to book entry securities collateral shall be governed by the law of the country in which the relevant 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

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

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

European banks envisage the following potential issues: legal use of security tokens as a guarantee; incomplete consistency among different EU states on the formal contractual requisites; and, in certain cases, EU countries cannot apply their national insolvency rules to financial collateral arrangements.

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.

One of the main effects of DLT-based trading will be to significantly shorten the settlement cycle, for example, by making the exchange of information meritorious and unalterable instantaneous. For this reason, the central clearing itself, if not adequately considered by the regulation (for example in reference to a certification system for the clearing of crypto-assets), risks not to be compatible with security tokens. However, a more detailed scenario heavily depends on a number of parameters, including the kind of DLT (permissioned or permissionless) and the kind/nature of the associated token.

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.

In our opinion, crypto-assets do not fall within the scope of EMIR's remit, as the Regulation applies only to derivatives.

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.

Considerations on transaction reporting (answer to Q.76) could be extended to reporting under article 9 of Regulation (EU) n. 648/2012. It's in particular difficult to report data required in table II sections 2.a and 2.b of Delegated Regulation (EU) n. 104/2017 and 105/2017. When the underlying of a derivative is a crypto-assets, regulated as financial instrument, the applicable regime should be provided for the financial instrument regardless of the technology used.

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.

Current rules can be considered technology neutral. That being said, clarification would be needed when taking into consideration that CCPs, CSDs, and TRs may not be necessary for a permissioned blockchain that is run solely by a group of financial institutions.

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.

European banks retain that, whenever possible, specific regulation should be issued and addressed to the underlying crypto-asset, not to the derivative built upon it.

9. The Alternative Investment Fund Directive

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

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

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

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

						Don't know /

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

For investments in security tokens the AIFM should choose a depositary able to operate as “custodian wallet provider”. As a consequence, credit institutions, investment firms providing the ancillary service of safe-keeping and administration of financial instruments will be encouraged to provide custodian wallet provider services. At the same time, however, there is still a high level of regulatory uncertainty on security token and their classification as financial instrument. Moreover, most of current depositaries don’t have the resources or knowledge in order to manage DLTs. The result could be a competitive advantage for depositaries able to manage blockchain and DLT, but also an obstacle for the growth of DLT and crypto-assets given the current lack of them and, therefore, the difficulty for AIFMs to purchase crypto-assets.

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.

Please consider the answer to Q.105.1.

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.

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.

The definition of transferable security is broad and goes beyond the examples of shares and bonds reported in MiFID II definition. Given the open nature of the definition, every crypto-asset traded on the exchange and purchased with investment purpose could be a financial instrument. In this uncertain context it's difficult to imagine UCITS Fund purchasing security-tokens.
As described for AIFM, the requirement to appoint a depositary and safe-keeping could be a competitive advantage for depositaries able to manage blockchain and DLT, but also an obstacle for the growth of DLT and crypto-assets given the current lack of them and, therefore, the difficulty for managers to purchase crypto-assets.

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.

Please consider the answer to Q. 107.1.

11. Other final comments and questions as regards tokens

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

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

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

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

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

Due to the technical user guidance, Q.108 needed to be answered to allow for this comment box. However, the EBF does not consider the question irrelevant, but is in favour of a market-neutral approach. Looking at the number of innovative solutions being developed in the permissionless world, the discussion of a regulatory approach requires careful consideration and continuous exchange of regulators and stakeholders.

On the one hand, regulatory flexibility for platforms operating on specific permission(less) models may allow platforms to include more market incumbents. On the other hand, permissionless DLT can pose challenges for financial institutions in terms of governance, scalability and efficiency. Banks respect their responsibilities under the existing regulatory framework, aiming at financial stability and consumer/investor protection. A consideration of regulatory flexibility should take note that viable technological solutions may not always fit into a simplified view of permissionless vs. permissioned category. Permissioned solutions can be developed within a permissionless network, using encryption and strong authentication. In turn, regulation should not base itself on labels and categories that may not reflect tomorrow's approach by the industries. The EBF supports an ongoing exchange to better understand the approach best suited to offer both market innovation and required legal certainty.
Generally, regulatory flexibility should not come at the expense of thorough risk management and should only be envisaged after a thorough risk analysis of all its potential impact.

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.

Permissionless ledgers can be considered an innovative and yet disruptive application of DLT, see also Q. 108.1. Supporting a technological-neutral approach based on the principle "same services, same risks, same rules", the EBF supports the regulators' attention to the phenomenon. The discussion requires careful consideration and continuous exchange of regulators and stakeholders.

Regulatory flexibility for platforms operating on specific permission(less) models may allow platforms to include more market incumbents. However, without centralized responsibilities and controls, permissonless blockchains inherit risks such as: money laundering, lack of liquidity, high volatility, credit risk (due to the possible lack of issuer information), disordered negotiations, delays in execution and settlement due to the behavior of miners, systemic risk, financial stability risk, settlement risk, settlement finality uncertainty, lack of liable and accountable party.

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

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

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

110.2 Please explain your reasoning for your answer to question 112:

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

Due to the technical user guidance, Q.108 needed to be answered to allow for this comment box. However, there are relevant comments to share. The current regulatory framework is inevitably based on the separation of trading and post-trading rules. In our view, after the uptake of DLT-based solution for post-trading services this will no longer be possible due to the concentration of processes and operations within the ledger: clearing activities and netting are will adopt real-time operations in the coming years, changing altogether the entire trading business.

However, this will mostly depend on the emergence of new business models and organizational arrangements between the various parties that will be using such new models. Any changes in that sense should be based on a deep risk/benefit analysis in view of the risks involved. Indeed, the risks associated with payment, clearing and settlement activities are in most instances the same, irrespective of whether the activity occurs on a single central ledger or a synchronized distributed ledger (CPMI, Feb 2017).

On a general note, the tokenization of assets will rely upon the currently established market credibility of trusted central authorities. To this extent, regulated entities are likely to be involved in the transitional period at the center between the chained and unchained sides of the trade.

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.

In light of fast-evolving technological approach and continuous dialogue with regulators and stakeholders across Europe, the EBF recommends continuing a careful evaluation of DLT evolution and its effects on business models on the financial market. Such dialogue will help to identify relevant issues, bringing together the important perspectives of relevant sectors, regulators and supervisors.

Question 112. Have you identified national provisions in your jurisdictions that would limit and/or constraint the effective functioning of DLT solutions or the use of security tokens?

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

112.1 Please provide specific examples (national provisions, implementation of EU acquis, supervisory practice, interpretation, application, ...) and explain your reasoning for your answer to question 112:

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

C. Assessment of legislation for 'e-money' tokens

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

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

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

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

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

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

113.1 Please provide specific examples (EMD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application, ...) and explain your reasoning for your answer to question 113:

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

Provided that a crypto-asset satisfies each element of the definition set out by the point (2) of Article 2 of the EMD2 ('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 as defined in point 5 of Article 4 of PSD2, and which is accepted by a natural or legal person other than the electronic money issuer'), the respective crypto-asset would qualify as 'electronic money'. In this case, authorization as an electronic money institution is required to carry out activities involving electronic money pursuant to Title II of the EMD2, unless a limited network exemption applies in accordance with Article 9 of that Directive.

However, discussions continue as to when payment tokens should qualify as e-money and which entities within the token architecture should be subject to the corresponding requirements. Tokens that are fully backed by fiat currency and are redeemable at par value at any time can qualify as e-money. The situation for stablecoins on the other hand appears less clear. Certain stablecoins – backed by funds segregated in bank accounts – could gain relevance as e-money, thereby being subject to the EMD. A stablecoin issued centrally, but only accessible to the user via a wallet account, could be different. In this scenario, it is unclear which, if any, of the entities involved are issuing e-money
In cases where stablecoins are issued by a depository institution, e.g. a bank, it could be argued that this crypto-asset constellation requires a treatment as bank deposit rather than e-money. Please consider the answer to Q.9. When a bank (or comparable deposit taking institution) utilizes DLT to evidence account balances denominated in a sovereign currency (or its fixed equivalent), it will not be altering the nature of the deposits as "money" and it will not be creating a separate instrument of value or medium of exchange from the sovereign currency. It would rather employ a different technology to record sovereign currency value on its books, therefore being rather an equivalent.

Following the principle "same services, same risks, same rules", crypto-asset-based transactions and entities issuing crypto-assets with a similar levels of risk as traditional e-money or payment transactions should not operate under different regulatory requirements. Payment users and consumers should not be put at risk.

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.

In accordance with the EBA Report on crypto-assets from 9 January 2019, the following considerations are important. 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 point (25) of Article 4 of the PSD2 unless they qualify as 'electronic money' for the purposes of the EMD2. Should a firm propose to carry out, using DLT, a 'payment service' as listed in Annex I to the PSD2 (such as the execution of payment transactions, including issuing 'payment instruments' and/or acquiring payment transactions and money remittance) with a crypto-asset that qualifies as 'electronic money', such activity would fall within the scope of the PSD2 by virtue of being 'funds'.

However, an e-money token could involve additional processes and risks, both technical (e.g. settlement delays) or due to financial complexities (e.g. special requirements on large reserves). Such processes and risks would need to be explained to payment users accordingly. Continuous discussions between regulators and stakeholders should address the question if the current transparency requirements under PSD2 are sufficiently capturing these new features and processes.

The access to account provisions included in PSD2 (articles 65-67) may not function as originally intended when applied to crypto-assets. The definition of an e-money token and appropriate assignment of responsibilities would need to be initially clarified, since the design of an e-money token may separate the emission of the e-money itself from the wallet account where detailed transactional information is held. The payments are actually initiated from the wallet account. If the latter is not considered to be an e-money account, this could mean that a user would not be able to share their full set of transactional information or initiate a payment through third parties.

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.

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.

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.

Safeguarding requirements under EMD2 require providers of such products to deposit customers' funds with commercial banks, or invest in high quality liquid assets, as a means to ensure the safeguarding of customers' funds. However, if such services are provided at a large scale - as would be the case with global stablecoins - this could imply a change in banks' funding structures, i.e. a significant proportion of retail funding would be replaced by wholesale funding, This would increase banks' funding costs. Furthermore, this pool of funds is likely to show greater mobility compared with retail deposits, which may reduce the stability of bank funding. In sum, this could eventually undermine the financial sector's role in financing long term investments, reducing the sector's capacity lend to the economy. In turn, this can negatively impact the effectiveness of monetary policy.

Prudential requirements (i.e. ongoing funds) might need to be fine-tuned to deal with the potential risks associated with the large-scale provision of e-money services that a systemically important stablecoin (global scope) could entail.

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