Contribution ID: c64bdcb6-42aa-4ee9-ac9d-63f08b95be48
Date: 13/03/2020 19:23:23

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

Jan Wolfgang

* Surname

Doser

* Email (this won't be published)

jan.wolfgang.doser@deutsche-boerse.com

* Country of origin

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

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

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

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

* Organisation name

255 character(s) maximum

Deutsche Börse Group

* Organisation size

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

Transparency register number

255 character(s) maximum

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

20884001341-42

* 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

* Publication privacy settings

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

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

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

☑ I agree with the personal data protection provisions

I. Questions for the general public

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

Question 1. Have you ever held crypto-assets?

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

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

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

II. Classification of crypto-assets

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

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

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

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

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

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

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

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

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

We need one single EU-classification which covers both: digital-assets, which represent the digitalized embodiment of an asset, and also crypto-assets, which are a subcategory of digital-assets. Hence, crypto-assets (like coin & token) are digital-assets based on cryptography, but other categories of digital-assets are imaginable. The classification should also refer to those services and activities related to these assets.

A clear and distinct categorization of digital-assets between security-, payment-, utility- and hybrid-asset is deemed of critical importance to determine if a given digital-asset falls under an existing EU regulative framework and to align the existing regulation.
Definitions should not be based on "technical" features only (e.g. cryptography), but on the value of the assets represented/embodied, if possible (meaning: if "digital securities" represent a "financial instrument" defined in MiFID II under Annex I, Section C of the MiFID II (1)-(11), then they should be treated as such instrument, e.g. if the embodied value is a share, then all rules for shares apply, if the embodied value is a commodity, then all rules for commodities apply).

A commonly, binding legislative approach, based on existing EU rules and regulations for the financial market would provide much a needed legal certainty to reduce regulatory arbitrage, inconsistencies and market fragmentation and to ensure scalability of services within the EU. This would place the EU as a global international standard setter, that embraces innovation.

Tech-neutrality and "same business, same risks, same rules" should apply to uphold the principles of transparency, fairness, stability, investor protection and market integrity.
It is important to have clarification by an actor on EU level, e.g. ESMA (in alignment with global standard setting bodies like ISO Technical Standards), that if digital-assets (like digital securities) qualify as a financial instruments due to their characteristics in a "substance over form" manner (see the MiFID II definition of financial instruments in the Annex I, Section C of the MiFID II), they will be subject to already existing financial rules.

This, would increase the speed to market for innovations, as market participants and authorities would act within a well-established legal framework and the rules are appropriate for institutional and retail investors.

If a hybrid-digital-asset contains elements of a financial instrument (at any point of its life-cycle), in principle, it should fall under the financial rules for the respective financial instrument.

Digital-assets, which are currently not covered by the current definitions of financial instruments (e.g. crypto-currencies) should be integrated in the MiFID II definition of financial instruments. We would propose to define a new category “other digital-assets” as a new point (12). This category could be defined in line with the definition provided for in the German Banking Act (KWG) for crypto-assets, which could act as a blueprint for the respective EU regulatory framework, see as an example: “Crypto-assets are defined as digital representations of value that are not issued or guaranteed by a central bank or a public authority, are not necessarily attached to a legally established currency and do not possess a legal status of currency or money, but are accepted by natural or legal persons as a means of exchange that can be transferred, stored and traded electronically or serve investment purposes other than e-money or a monetary value used in limited networks for certain exempt electronic payments processed by telecommunication providers.“

Please refer to, the German KWG definition and also the ISO TC 307 „Blockchain and distributed ledger technologies – Terminology“.

Utility assets which do not fulfil the criteria above, should still be treated in such a way that investors are protected and markets are fair, efficient and transparent
(see e.g. IOSCO objectives of Securities Regulation: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwioybC1z_7nAhXJUJoKHVklAHEQFjABegQIChAE&url=https%3A%2F%2Fwww.iosco.org%2Flibrary%2Fpubdocs%2Fpdf%2FIOSCOPD154.pdf&usg=AOvVaw1QZuFy_iuLk2_IBNKNQ49A).

Please see also Q 6,7 and 8 on the definition of digital money.

Question 6. In your view, would it be useful to create a classification of crypto-assets at EU level?

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

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

Please explain your reasoning:

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

We do not favour “soft law” (e.g. guiding principles), which might be interpreted differently by Member States and with future EU-rules passporting should be possible. (see answer to Q5)

Further, level 2 regulatory technical standards (RTS / ITS) by an actor on EU level (ESMA) towards the legal qualification of types of digital-assets (compared to other financial instruments already established in the market) would be helpful.

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.

To differentiate such categories we refer to the BaFin and ISO classification, which provide a good approach.

In your paper you refer to (global) stable coins. Digital payment assets (payment tokens) or “digital money” in our view have different subcategories, depending on certain features like the openness of the network and governance structure used (public or private ledger, permissioned or permissionless), the backing or the reserve (no backing or backing by assets) and the issuer. This would result in the following classification (illustrative):

a) Crypto-currencies: native tokens which have no issuer, usually running on a public/permissionless ledger; example: Bitcoin
b) Stablecoins: issued by a private non-financial company, backed by asset(s), on a private or public ledger; example: Libra
c) Digital bank money: issued by financial institutition with banking license, additional backing with assets is optional, usually on a private/permissioned ledger; example: JP Morgan Coin
d) Central Bank Digital Currency: issued by central bank

Digital payment assets should fall into the new class “other digital-assets”, as long they are not covered by other existing legislation like EMD2 or PSD2 (Q8).
For further details on the differentiation of payment tokens (also "virtual currency", "payment token" or "bare-bone token"), utility tokens and security (similar) tokens ("equity token", "security token", "investment token" or "asset token") as well as hybrid forms refer to the respective BaFin Merkblatt (link: "https://www.bafin.de /SharedDocs/Downloads/DE/Merkblatt/WA/dl_wa_merkblatt_ICOs.pdf?__blob=publicationFile&v=1 Page").

Please refer also to the answers of Questions 5,6,7 and 8.

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.

Please refer also to the answers of Questions 5 and 7.

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 your paper you refer to (global) stable coins. Digital payment assets or “digital money” in our view have different subcategories, depending on certain features like the technology used (public or private ledger, permissioned or permissionless), the backing or the reserve (no backing or backing by assets) and the issuer. This would result in the following classification (illustrative):
a) Crypto-currencies: native tokens which have no issuer, usually running on a public/permissionless ledger; example: Bitcoin
b) Stablecoins: issued by a private non-financial company, backed by asset(s), on a private or public ledger; example: Libra
c) Digital bank money: issued by financial institution with banking license, additional backing with assets is optional, usually on a private/permissioned ledger; example: JP Morgan Coin
d) Central Bank Digital Currency: issued by central bank

In our view, a privately issued wholesale stablecoin could be seen as an “intermediate” solution before a Central Bank Digital Currency is available.
For more information please refer to the Bundesbank website (BLOCKBASTER). (link: "https://www.bundesbank.de/en/press/press-releases/deutsche-bundesbank-and-deutsche-boerse-successfully-complete-tests-for-blockchain-prototypes-764698").

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.

The consequence of such definition may be the application of a deposit guarantee scheme, i.e. in the event of a default of a crypto-custodian the investors would benefit from a bank deposit guarantee fund to which the relevant banks (crypto-custodians) would be required to pay contributions to. This would enhance consumer protection, but put additional burden on crypto-custodians.

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.

None.

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.

No DBG response.

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.

Beside „classic“ risks of new asset-classes (fraud, money laundering, market manipulation …) technology related „new“ risks arise (energy consumption, finality, integrity of the network, „forks“, „whales“, „right to be forgotten” in Art 17 GDPR not easy to apply…).

Some DLT forms, such as public blockchains have no legally accountable entity to be held liable for failing to implement risk management procedures to address the risks mentioned above, which is a risk by itself. We would recommend policies and procedures to be followed by entities that wish to offer their products and services to “retail clients” or offer securities to the public.

There are specific risks arising from smart contracts e.g. in the case of unintended programming of the algorithm within such a smart contract. A so called "trusted third party" (see Q35) would help to prevent or mitigate such risks from occurring.

So-called smart contracts should ideally follow a general standard. Such standards could be set at the EU level, but should be aligned with international bodies and developed with market participants.

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.

Beside „classic“ risks of new asset-classes (fraud, money laundering, market manipulation …) technology related „new“ risks arise (energy consumption, finality, integrity of the network, „forks“, „whales“, „right to be forgotten” in Art 17 GDPR not easy to apply…).

From our point of view, these “new” types of digital assets could pose the “classical” risks of new markets to consumers and market integrity. Effective regulatory frameworks have been put in place after the financial crisis, to deal with such risks.

This regulatory framework should apply to services related to digital-assets as well. Specific risks attached to such services (e.g. IT-related risks as mentioned in our response to question 11.1) should be thoroughly assessed and addressed by appropriate future regulatory requirements.

Some DLT forms, such as public blockchains have no legally accountable entity to be held liable for failing to implement risk management procedures to address the risks mentioned above, which is a risk by itself. We would recommend policies and procedures to be followed by entities that wish to offer their products and services to “retail clients” or offer securities to the public.

Further, there is a legal risk as to the ownership and insolvency remoteness of holdings which particularly applies to crypto-currencies, since these do not have an issuer and are digital units only. It is questionable,

whether ownership may derive from the possession of private keys only, specifically if custody chains with intermediaries are being used. Also, settlement finality is unclear when “over-taking” blocks are being hashed.

There are specific risks arising from smart contracts e.g. in the case of unintended programming of the algorithm within such a smart contract. A trusted third party would help to prevent or mitigate such risks from occurring.

So-called smart contracts should ideally follow a general standard. Such standards could be set at the EU level, but should be aligned with international bodies and developed with market participants (see Question 11).

We as DBG are part of ISO/TC 307/WG2 which deals with smart contracts, we are also aware of and closely monitor ISDA`s Legal Guidelines for Smart Derivatives Contracts. At EU level CEN-CLC-JTC19 blockchain and Distributed Ledger Technologies are the responsible standard setting bodies.

“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.

(Global) Stablecoins bring the payment element to distributed ledger networks. This potentially enables 24/7, real-time, “delivery-versus-payment” exchange of digital-assets against digital cash within DLT; on top, “payment-versus-payment” in different currencies becomes feasible.

The value of stablecoins, however, very much depend on the credit quality of their issuer and/or the quality and accessibility of the reserves held by the issuer (‘collateral’, like securities, bonds, currencies).

Ideally, stablecoins should be pegged 1:1 to a fiat currency and reserves kept in an insolvency remote way. Especially, for the wholesale market the quality of stablecoins must be at least like the quality of fiat money in relevant legacy systems.

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.

Price/value stability: i.e. the risk that the value of the stablecoin fluctuates depending on the credit quality of the issuer (e.g. the probability of the default of the issuer) and the "reserves" ("collateral", i.e. the assets collected as "reserves") and their accessibility.

The issuer of the coin as well as the operator of such a DLT-system need to be trustworthy and reliable parties – ideally neutral bodies that reduce potential conflicts of interest related to other businesses they carry out. Therefore, we would endorse to use trusted third parties with accounts on central bank level.

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.

Global stablecoins could represent a much higher volume than stablecoins and might therefore influence financial stability. Likewise, the management of the reserve pool of a global stablecoin can have strong influence on prices and the functioning of markets for the particular assets.

As a conclusion central banks should be involved in the development as well as in the regulatory framework /oversight.

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

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

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

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

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

We advocate to incorporate digital-assets into the existing European financial regulatory framework (e.g. all digital-/crypto-assets that are to be regarded as financial instruments in the MiFID II sense) instead of creating a bespoke regulatory regime. Existing regulation should be supplemented where required to address technology related “new” risks. This would provide for legal certainty for market participants as they ensure for high standards of investor protection and market integrity.

A new regime is not necessary. As of now, from our point of view this would only be the case for those utility digital-assets which have only value according to the trading participants (cf. definition of crypto-assets pursuant to section 1 para. 11 sentences 4 and 5 of the German Banking Act "crypto-assets are defined as digital representations of value that are not issued or guaranteed by a central bank or a public authority, are not necessarily attached to a legally established currency and do not possess a legal status of currency or money, but are accepted by natural or legal persons as a means of exchange that can be transferred, stored and traded electronically or serve investment purposes other than e-money or a monetary value used in limited networks for certain exempt electronic payments processed by telecommunication providers.”

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

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

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

On 29 November 2019, the German legislator introduced a new regulatory framework for crypto-assets. As part of the transposition of the Fifth EU Money Laundering Directive into national law, the German legislator amended the German Banking Act (Kreditwesengesetz – KWG) to provide legal clarity regarding crypto-assets (cf. Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, BGBl. 2019 I, p. 2602, for the legislatory process see "https://dipbt.bundestag.de/extrakt/ba/WP19/2517/251728.html").

As of 01 January 2020, crypto-assets are classified as financial instrument under the German Banking Act. Therefore, entities which provide services with respect to crypto-assets, are required to be licensed by BaFin. This also holds for crypto-custody services.

The German legislator defines crypto-assets as "(…) digital representations of a value: 1) that has not been issued or guaranteed by any central bank or public body and does not have the legal status of currency or money, 2) is accepted by natural or legal persons as a means of exchange or payment by virtue of an agreement or actual practice, or is used for investment purposes and 3) can be transferred, stored and traded electronically."

E-money and monetary values within the meaning of the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz – ZAG) are expressly excluded from the scope of such defined crypto-assets.

As explicitly laid out in the recitals (BR-Drs 352/19, p. 122), the new term of crypto-assets serves as a catch-all provision. Therefore, if a crypto-asset also qualifies as a security, the provisions on securities will be applied primarily. The crypto-asset specific provisions therefore will only be applied to those crypto-assets that do not fall into the scope of other financial instruments.

With this decision to, the German legislator follows the principle „Same business, same risk, same rules", i.e. financial instruments are, in principle, regulated in a technology-neutral approach, but, to provide a holistic regulatory landscape, other crypto-assets that do not fall into the scope of any 'classical' financial instruments are now also included into regulation. DBG considers this as a sensible approach as it strikes an appropriate balance between an innovation-friendly environment, while maintaining high investor protection standards. The incorporation of crypto-assets into already existing regulatory framework appears internationally the prevailing approach. For example, other Member States, such as France and Malta, have enacted similar regulatory frameworks as Germany.

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.

DBG supports the aim to create a harmonized regulatory framework for crypto-assets and crypto-asset service providers in the EU. A common framework across all Member States would provide market participants with the legal certainty they need to reduce their costs for compliance and ultimately harness the advantages of the internal market as the current trend to differing national legislation of crypto-assets (see Germany, France) could be stopped or reverted.

The German regulatory approach towards crypto-assets has shown that legal certainty for market participants can be most effectively achieved by incorporating crypto-assets into the existing financial regulatory framework that provides for a high standard of consumer protection and market integrity. This creates a level playing field for all market participants. Moreover, it allows for innovation, while taking investor protection concerns serious.

DBG therefore advocates to incorporate digital-/crypto-assets into the existing European financial regulatory landscape instead of creating a bespoke regulatory regime.

This creates a level playing field for market participants and allows for innovation, while taking investor protection concerns serious.

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.

Please, provide clarity as to the prudential treatment of financial institutions´ exposures to digital-assets aligned with BIS/Basel Committee.

We would prefer binding regulation to have clarity due to a common framework.

With regard to the (capital) requirements, a distinction has to be made between closed/private environments and those digital-assets which are offered to the broader public:

We are of the opinion that the conditions for separate prudential treatments should directly relate to the core of the meaning of “(macro-)prudential”:

If digital-assets are offered to a wide audience/public without access restrictions and qualify as a financial instrument, as an investment asset-class, it should be treated following the principle “same business, same risk, same rules”.

Otherwise, if digital-assets are more comparable to a “technical solution” used in a closed environment (with restricted access only), than it should be treated differently.

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.

See above.

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.

Binding EU-provisions on the transfer of digital-assets and digitalization of tangible assets would greatly help to achieve an EU-market in respect of a token-based economy. A common EU-approach would solve the issue of the applicable law with regard to content and requirements in the national jurisdictions. Please refer also to the IOSCO report “Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms”
Yes, it should be ensured that in transfers of ownership of digital-assets are possible under each national member state rules, i.e. by agreement and booking in a suitable custody system.
Harmonisation of the laws on digital-/crypto-assets transfer and tokenization of tangible assets would greatly help to achieve an EU international market in respect of a token-based economy. Any harmonization would contribute to solve two issues: (i) the issue of the applicable law and (ii) the issue of the content and requirements of the applicable law.
Although different legal positions (property, contractual positions, etc.) may be tokenized, for the sake of simplicity, the following shall only focus on aspects regarding the tokenization of physical assets as implied by the question. For the tokenization of other legal positions, the remarks below may be applied mutatis mutandis.
(i) The issue of the applicable law
In respect of property law, the applicable law is normally based on the lex rei sitae principle, i.e. the law where the property is situated will be applied. However, when applying this principle to crypto-assets, it gives rise to a number of serious questions that lead to legal uncertainty: First of all, other than for physical assets,

the place where a crypto-asset is situated may not be determined with sufficient certainty: is it the physical place where to tokenizer was situated in the second the tokenization took place (and if yes, how could this be proven?), is it the physical place where the nodes are situated on which the ledger is run?, is it the physical place where the owner of a private key corresponding to a crypto-asset is situated?
These issues are potentiated when one takes into account custody chains, that are, at least in respect to securities, normally governed by the place of the relevant intermediary approach, which effectively leads to multiple changes of the legal nature of the assets under custody, in case the different persons taking part in the custody change are based in different jurisdictions. As also for crypto-assets multiple custody chains are likely, this topic will arise here as well.
By harmonizing national civil laws, the question of the applicable law and how it is determined for crypto-assets should also be addressed in a uniform way.
(ii) The issue of the content and requirements of the applicable law
The legal concepts of ownership and the requirements of its transfer differ considerably, even if only the laws in respect to physical assets are taken into account. Even today, this creates an obstacle for the EU internal market because a rational investor needs to assess the legal position that comes with the concept of "property" in the respective country and the requirements for a transfer of such property before making any investment decision in an unknown jurisdiction. This process is burdensome, but since the legal concepts with respect to physical assets are well known within a certain jurisdiction, at least manageable.
For crypto-assets, the situation is different: Until now, most countries do not have clear rules addressing the legal concept of crypto-assets. Thus, under most jurisdictions, it is currently simply not possible for an investor to assess the legal position that may be achieved by holding a crypto-asset, or to assess the requirements to validly transfer a crypto-asset from one person to another.
We expect that jurisdictions interested in taking part in the digital-asset economy will develop concepts to address the legal position in crypto-assets and the transfer requirements shortly. We anticipate that each jurisdiction will base any new concepts they will apply to crypto-assets on their respective concepts that currently exist in respect to physical assets. Consequently, not harmonizing national civil laws with respect to the tokenization of physical assets and the transfer requirements will deepen the fragmentation that currently exists with respect to national property laws.
When harmonizing the civil laws, one should also address specific issues that only arise with respect to crypto-assets such as: how to determine the 'owner' of a crypto-asset – is it only the holder of a corresponding private key or rather the initiator of the private key creation? When is a transfer of crypto-assets legally considered as final (taking into account technical specifics of the used ledger such as probabilistic finality-based ledgers).

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.

No DBG response.

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.

A physical presence of issuers and sponsors of digital-assets marketed to EU investors is not necessary, if digital-assets are covered by the definition of financial instruments and financial services, as EU-equivalence rules would apply, or national competencies would ensure investor protection.

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.

It is crucial to require a standardized information set from issuers or sponsors of digital-assets, which informs the public on digital-/crypto-assets based on specified criteria. However, it needs to be acknowledged that not every digital-asset has an identifiable issuer or sponsor (e.g. most crypto-currencies do not have an issuer, while other digital-assets might have an issuer).

DBG generally considers it crucial to require from issuers or sponsors of digital-/crypto-assets a standardized information set, which informs the public based on to be specified criteria about the digital-/crypto-asset.

However, it needs to be acknowledged that not every digital-/crypto-asset has an identifiable issuer or sponsor. The most prominent example of such a crypto-asset is Bitcoin where a whitepaper only has been provided under a pseudonym. In these cases, the entity which places the digital-/crypto-asset on the market could be a potential provider of a standardized information set.

In addition, it should be noted that the information that is currently normally provided in a whitepaper for a digital-/crypto-asset normally does not meet the high standards for customer protection as required for financial instruments for example under the EU Prospectus Regulation. Therefore, it should be made clear that the prospectus requirements as currently set out under EU law shall also apply to crypto-assets.

Any group of actors that are involved in the public offering of these assets, need to inform potential investors. This should be achieved by the requirement of publishing a respective risk profile and additional information on the rights and risks that are embedded into such an offering

As long as digital-/crypto-assets have a function as defined above (see Question 5 and 14), a public offering of such assets should be regulated for the protection of the public.

We therefore assume that all assets belonging to this definition are "financial instruments" and all services provided to third parties with these instruments are financial services.

Therefore, there should be a requirement for those financial institutions that are involved in the public offering of these assets, to inform potential investors so that they can are able to make an informed decision about the value of these assets.

This may be achieved by the requirement of publishing a respective risk profile and additional information on the rights and risks that are embedded into such an offering.

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.

One could consider whether all prospectus information may be contained in a token or whether this would be too intransparent (may not be read by consumers) and these would need to be more easily accessible for investors (in readable file format, as today).

BaFin has already issued a guidance notice on prospectus and authorisation requirements for crypto-tokens (link: "
https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_wa_merkblatt_ICOs_en.pdf?__blob=publicationFile&v=4")

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.

No DBG response.

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.

Art. 3 and 49 CSDR are of relevance only in case of trading of digital-/crypto securities on trading venues.

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.

See above.

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.

We would propose the following criteria to distinguish stablecoins from global stablecoins: number of currencies included (coin itself and/or reserve pool); number of participants and volumes of coins issued as well as the underlying assets´ insolvency regimes.
To address the mentioned risks, the issuer and/or system operator should ideally be authorized and supervised companies. A strong rulebook should be required including clear and transparent rules for the management of the reserve (e.g. fiat-money only, no cross-currency risk etc.).

Additional requirements for the issuer and/or manager of the reserve should be: Assets of the reserve should be kept at a central bank (cash) or regulated/supervised institutions (CSD, custodian); assets of the reserve should be highly liquid, with limited market and credit risk; prudent risk parameters should be applied for the reserve; e.g. composition of reserve (cash vs. securities), concentration risks, definition of volume caps per currency, ratios of asset classes amongst each other; if reserves in cash, then ideally held with central banks; if with commercial banks, then risk diversification required i.e. limited amount per bank.

To address specific risks of stablecoins and global stablecoins a limitation in the geographical spread

through underlying regional networks might be helpful.
All risks mentioned in Q13 are particularly valid for global stablecoins and must be managed adequately as nearly all of them define necessary clear attributes and must haves of a global stablecoin. Simplified, one could reduce a possible distinction to the following factors: 1) Number of currencies (coin itself and/or reserve pool) 2) Number of participants (reach) 3) Volume(s) of coins(s) issued. The insolvency remoteness of the backed assets' ("reserve") will be a crucial factor for investors.

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.

Ideally, all measures that allow a more “passive” management of the reserve (e.g. fiat-money only, no cross-currency risk etc.) and the trustworthiness of issuer and/or system operator combined with a strong rulebook.

Assets of the reserve should be highly liquid, with limited market and credit risk.
Prudent risk parameters should be applied for the reserve; e.g. composition of reserve (cash vs. securities), concentration risks, definition of volume caps per currency, ratios of asset classes amongst each other.

If reserves in cash, then ideally held with central banks; if with commercial banks, then risk diversification required i.e. limited amount per bank

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.

To make a stablecoin "really" stable the stability of the reserve pool must be granted at all times.

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.

A limitation in the geographical spread can only arise through the underlying network of a token / coin. Therefore, global coins are available on global networks and regional network carry regional coins. If the distribution of the network of coins crosses the borders of jurisdictions, the rules that also apply to securities in cross-border securities transactions must be applied. Ideally, the same rules should apply within the EU and the information provided in a public offer in one EU country should also be acceptable in another (passporting).

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.

See also response above.

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

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

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

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

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

It makes sense to differentiate between wholesale and retail clients. The end customer (retail investor, consumer) needs a higher level of protection than a professional investor (financial institution or selected client of a financial institution).

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.

Digital-assets should be traded on trading venue as defined in MiFID II only, i.e. “regulated markets”, MTFs or OTFs. Consequently, all the respective rules should apply.
For trading platforms a proper way of price formation in multilateral trading and price dissemination should be ensured to a level, that investors can find a price orientation to a certain regulatory standard.

Under MiFID II, besides transparency, liquidity provision through market maker is a key topic to ensure orderly price formation (under stressed market conditions). This could be relevant for trading of crypto-assets on trading venues.
Regulation should ensure that there is no difference between trading against fiat money or trading against other regulatory-compliance digital-assets (for example due diligence check, public-address check…).

Price formation needs to follow proper rules and should have an appropriate level of pre- and post-trade transparency. Exemptions and waivers should be granted by national competent authorities which consult with ESMA, like today.

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.

Digital-/crypto-assets are values that base only on a new technology. When being financial instruments, they serve for the same purposes as current financial instruments. Therefore, we believe that they have to follow the same rules.

With a view to trading of securities on a trading venue, Art. 3 CSDR is referring to book- entry form as immobilisation or a direct issuance in dematerialised form. When digital-/crypto-assets qualify as financial instruments (cf. also the definition of crypto-assets pursuant to section 1 para. 11 sentences 4 and 5 of the German Banking Act), they should be (multilaterally) traded only on trading venues according to MiFID II. The rules might have to be amended, to address additional risks specifically attached to digital-/crypto-assets). Under MiFID II, multilateral trading of financial instruments is possible on regulated markets, MTFs and (for bonds, structured finance products, emission allowances or derivatives) on OTFs.

Access to trading venues and thus to trading shall like as to date have financial services companies as intermediaries. All services, especially such as sending an order and safe keeping of crypto-assets are provided by these; under the German Banking Act, the latter case is a new financial service that requires a new form of license (crypto custodian – if not crypto-securities).

Settlement of transactions executed on trading venues and safekeeping of the crypto-assets would take place in a crypto-custodian, similar to the way securities are held in the CSD today. If such a model is implemented, all of the above dangerous outcomes could be mitigated.

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.

In order to prevent conflicts of interest, money laundering, financing of terrorism intermediaries must be held responsible for those issues. Fraud is one of the predicative offences for AML. Standards on crypto-currency should be aligned with the standard for fiat-currency in order to have competitive systems in place and to avoid being easily misused for money laundering.

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.

Digital-assets are to be divided into different classes: digital securities and digital payment assets, including crypto-currency assets (See above Q5/Q8). The latter is e.g. Bitcoin.

The new to be developed rules would apply to payment asset. All the existing securities rule sets should apply to digital securities. In the case of digital securities, we always assume that Art. 3 CSDR requires securities traded on a trading venue to be held in accounts at a CSD. Even if they are issued and held on a private DLT solution. So that some of the problems (AML, fraud, conflict of interest etc.) mentioned cannot arise.

In the case of digital-/crypto-assets, in the category of digital-payment assets that are not securities, access to the regulated area must be secured by intermediaries against money laundering etc.

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.

Risk of absence of accountable entity in the EU is a problem, as we need aligned standards across the EU rather than standards by country.

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.

So-called “crypto-currencies/asset exchanges” should have to follow the same rules applicable to trading venues (e.g. accountability, operational resilience / ICT security, recordkeeping). In order to apply all benefits to all types of trading of financial instruments no differentiation between crypto to crypto vs. crypto to fiat should be made.

All market participants should act with a respective authorization and/or set of licenses according to their activities / services, e.g. payment, execution of security transactions at an MTF, safe keeping of digital-assets, safekeeping of securities, organizing a multilateral trading facility etc.

Crypto-asset exchanges (as multilateral trading platforms in financial instruments) have to follow the same rules as described above. In order to apply all benefits to all types of trading of financial instruments no differentiation between crypto to crypto vs. crypto to fiat should be made. All involved participants are acting as financial service companies with a respective set of licenses, such as: payment, execution of security transactions at an MTF, safe keeping of crypto-assets, safe keeping of securities, organising a multilateral trading facility etc.

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.

It should not be allowed to transfer digital-assets including digital money from and to anonymous accounts without any onboarding or KYC requirements. Without a clear identity of the account holder, proxy and beneficial owner (similar to bank accounts for fiat- currency) there is a high exposure for money laundering.

Wallet provider should be regulated and falling under the AMLD and their national transposition, to create and ensure trust in the digital and crypto market. Further guidance on AML/KYC handling of accidental /unintended transfers is also needed, given the irreversibility of transactions esp. on public chains.

There is legal uncertainty with respect to the allocation of ownership as regards the holdings in a wallet, if this is not provided for by law (holders of private keys could qualify as quasi-owners of the relevant digital-assets, but this would not be appropriate for a multi-level holding custody structure).

Also, please clarify under which conditions material outsourcing with regard to digital-asset custody would be allowed (e.g. counterparty risk, standards, IT security etc.).

To ensure the integrity of the financial markets and mitigate risks, custodial wallet providers for the provision of custody are obliged entities and have to comply with the fifth AMLD (Art 1, (2) (d) (19). Further, they should be licensed as financial service providers, e.g. rules pertaining to the German "crypto custody business", which was defined recently as financial service in the KWG.

We see that custody solutions have been developed on the market already and might not be rebuilt by incumbent companies, but instead a lot of them will partner with technical or business custody providers. This leads to material outsourcing. It should be clarified under which conditions material outsourcing regulation fits the needs of digital-asset custody (counterparty risk, insurances, standards and IT security etc.).

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.

See above.

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.

No DBG response.

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.

Custodians and CSDs should be explicitly allowed according to CSDR to hold any kind of digital-asset in appropriate custody systems.

There has to be clarity in determining when crypto-currencies are compliant with regard to AMLD. Limitation of what source of crypto-currency should be accepted in terms of “when is a currency compliant with regard to AML. E.g. usage of Tumblers, from sanctioned or FATF countries, what is the maximum historic information of a currency that needs to be considered as suspicious (e.g. a maximum of 3 former transactions with this specific currency for AML and Sanctions monitoring).

Since digital utility assets may evolve into digital hybrid securities, at any given time, all kind of digital-assets should be “custodizeable” within a CSD or custodian bank

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.

Yes, provided that custodial wallet providers are compliant with all applicable rules as regards the custody of financial instruments. In any case, CSDs and custody banks holding financial instruments should be allowed to also hold digital-/crypto-assets.

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.

We prefer the following definition from the AMLD for wallet provider: „A custodian wallet provider means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer cryptographical and other digital-assets“ The custodian wallet provider was already a defined term under AMDL and is considered a new “obliged entity” and therefore should be regulated.

We would advise to regulate the digital-/crypto-asset custody business compliant with all relevant custody rules that govern traditional securities business (e.g. AIFMD/UCITS, CSDR, EMIR, etc.).

For example, if crypto exchanges hold crypto-assets for a certain period of time, they should also be compliant with all relevant custody rules, in order not to create fractions in the market.

A trusted third party builds a bridge for the exiting financial instruments in the “traditional world” via DLT solutions (see Q35.2)

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.

Digital-/crypto-assets can also represent securities which have to process different events in the life cycle. For example, dividends, voting rights, interest rates, other corporate actions and capital measures. Such events are implemented by so-called smart contracts and should ideally follow a general standard. Such standards could be set at different levels (EU, national, market) and should be controlled by central bodies (supervisory authorities, stock exchange, CSD) in case of newly issued assets. In any case, it is important that these events are carried out in accordance with the applicable laws and regulations. This would ensure investor protection and would deal with the unresolved issue of liability (who will be responsible, if things go "wrong"). Similarly, information that triggers such events should only be sent by authorized agents on the DLT/blockchains (Smart Oracle).

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.

Further requirements are needed for services which are similar to those already regulated on EU level e.g. by Annex I A of MiFID II, like the 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 (or services defined in CSDR, EMIR or AIFMD).
To comply with those requirements a trusted third party is always needed in the financial industry to create trust in the market.

A trusted third party builds a bridge for the exiting financial instruments in the “traditional world” via DLT solutions, in other words “ OFF-Chain to ON-Chain bridging”. Further, it guarantees the substance of a token, which is backed by financial instruments that is kept off ledger/chain
In our view, trusted third parties will play the role of a gate keeper for future native digital assets, which will be issued directly on the chain. The trusted third party will check standards for admission and the eligibility of an asset on chain: e.g. it will check if the asset is a security and transform it to a security token.
Another role that the thrusted third party will play would be to check smart contract codes (programable deterministic language), that could be in the form of assessing adherence with international standards ISO in general ISDA for Derivatives (ISDA Master Agreement) /ICMA (Repo).
A trusted third party is always needed in the financial industry to create trust in the market; also it holds high responsibility, especially to address following functions such as: 1) Control access/admission 2) Set rules for the participating nodes 3)Address potential conflicts of interest and KYC and AML requirements 4) Apply risk management 5) Be reliable for market integrity, security and other regulatory requirements
For example, HQLAx , a DLT based financial technology innovation firm, uses a trusted third party, which is complying with the existing respective rules, which adds trust. (https://www.hqla-x.com/) In the case of

HQLAx the trusted third party creates the token on the DLT that represents the ownership of the security on a given basket. The trusted third party currently is operating under a CSSF Professionals of the financial sector (PFS) licenses.
Furthermore, from our point of view, a trusted third party can be defined as an entity, which is following all the respective rules and holds all the necessary licenses and is authorized, irrespectively of the specific industry it is operating in.

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.

No DBG response.

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.

The biggest market integrity risks related to the trading of digital-/crypto-assets are AML/countering the financing of terrorism, consumer / investor protection as well as supervision and oversight of digital-assets service providers. These aspects must be considered, due to their important role in making the new asset class trustworthy, secure and successful.

We want to highlight that the mentioned risks could be most effectively be addressed by integrating trading platforms and exchanges for digital-/crypto-assets into the MiFID II framework for trading venues, which would require them to employ anti-manipulation and trading surveillance measures.

The more effective those issues are addressed, the easier it is for (institutional) investors to invest and help the market to develop (size, liquidity, professionalism).
It is time to bring the digital-asset ecosystem to the same level of regulation as other asset classes.

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.

Please see above.

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.

Please see Q37.

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.

With regard to onboarding and KYC not the supervisor but the wallet provider should have the obligation. Wallet provider and trading platforms should be able to identify the parties to transactions in digital-/crypto-assets. This might be easier to control and monitor using private permissioned chains.

CCPs as trusted third parties as today would deliver an efficiency gain.
If is there is a clearing obligation for these assets, CCPs would do the reporting and know the relevant parties (at least clearing members, but not necessarily their clients depending on the clearing model). Further, CCPs are well placed to process the end to end lifecycle and step in as central counterparty.

Further, if digital-/crypto-assets are concerned that qualify as financial instruments and are traded on a trading venue, Art. 25 (2) MiFIR would apply that requires operators of trading venues to identify the customer of the trading member (not necessarily the end customer) that is party to a transaction and to keep this information at the disposal of the competent authority for at least 5 years.

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

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

Question 40. Provided that there are new legislative requirements to ensure the proper identification of transacting parties in crypto-assets, how can it be ensured that these requirements are not circumvented by trading on platforms/exchanges in third countries?

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

Regulatory framework under MiFID II/MiFIR: either requirement for third-country firms that want to offer investment services to EU customers, including the operation of an MTF/OTF, to obtain a license within the EU or admission of such services to institutional customers based on an equivalence decision. For third-country exchanges, need to obtain license in Member States from which trading members will be admitted to trading.

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.

To create trust in the crypto market and in order to enable intermediaries and banks to sustainably invest into this business this is of utmost importance. Financial service providers ensure AML/KYC and secure that only "unsuspicious/compliant" tokens are in circulation.
The more crypto-currencies/assets are used for regular transfer of wealth/means of payments, the more important it will be to avoid money laundering and any violation of sanctions regimes.

Therefore, the same rules should apply than for fiat-currency (AMLD5) and wallet providers should be subject to this act and be handled as financial institutions from an onboarding and KYC perspective.

Clear rules are required to determine the level of monitoring for KYC/AML in the general context of blockchain, especially for public permissionless blockchains, since there is all historical information stored with the currency but identification / translation of this historical information is partially impossible/difficult and the depth of monitoring should be limited to e.g. a reasonable amount of previous transactions.

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

Question 42. Beyond fiat-to-crypto exchanges and wallet providers that are currently covered by the EU AML/CFT framework, are there crypto-asset

services that should also be added to the EU AML/CFT legal framework obligations?

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

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

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

Please see above.

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.

A trusted third party would help in a bespoke framework to bring trust in the market (see Q35).

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.

Trusted third parties would help in a bespoke framework. OTC business needs to be cleared and settled in order to address risks. Please see also our approach to go for an obligation to trade digital-/crypto-assets on trading venues.

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.

As outlined above only adequate handling of crypto-currency (same as fiat-currency) will help creating trust in this new business and avoid misuse of intermediaries / banks / wallet providers for AML / sanctions.

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.

Regulated entities such as CCP and CSDs are only able to do business with intermediaries, wallet providers etc. if they are trustworthy, apply state of the art AML and sanctions framework including fraud detection, conflicts of interest management and applying a code of conduct.

Depending on the risk, there should be a requirement for providers of services related to digital-/crypto-assets to register with the competent authorities, while licensing requirements should only apply depending on the degree of risk exposure. A EU harmonized approach would be helpful.

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.

If digital-/crypto-assets are handled as securities then the issuer/broker should be obliged to issue/distribute similar information as with any other security (customer information on product and associated risk).

It should be determined for which customer the product is suitable (from a risk perspective as well as from a professional background perspective).

Smart contracts should be transparent for consumers.

Wallet providers, issuers of tokens and those "selling them" have to highlight certain risks. For advising clients, you have to follow the relevant rules as of today, have the adequate licenses and therefore need to advise on risks.

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.

As said above, sustainable business can only be done if there is trust in the market. As all other means of regulations are mainly addressing the “trust” issue there is no need to handle digital-/crypto-assets different from any other asset.

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.

Yes, but it needs to be carefully monitored, as any digital utility-asset may evolve into a hybrid-security asset which would then be out of scope.

For an example, a voucher of a company becoming fungible/tradable, e.g. as a means of payment.

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.

Yes, as it is today for securities: if educated investor than professional standard; lower standards than for retail, dependent on professionalism of investor. No reason not to apply already existing regulation for securities/assets.

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.

It should not be allowed to transfer digital-assets including digital money from and to anonymous accounts without any onboarding or KYC requirements. Wallet provider should be regulated and falling under the AML and their national transposition, to create and ensure trust in the digital and crypto-market.

Further guidance on AML/KYC handling of accidental/unintended transfers (e.g. air drops) is also needed, given the irreversibility of transactions esp. on public chains. Here industry standards (like in securities markets) could apply that the receiver needs to confirm that he accepts the delivery.

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.

Same as with other securities/currencies. Individual or regulatory assessment of the country and their means of investor protection in order to determine whether to be accepted or not. Specifically, there must not be a certain waiver or exemption of any kind for crypto-assets with regards data protection laws (the right of deletion cannot be waived due to technological limitations).

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.

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.

We would see the need to apply the existing supervisory structures due to specific character of digital-/crypto-assets, the “substance over form” principle should apply.

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.

Beside the usual tools, more IT-knowledge and expertise e.g. how smart contracts are programmed would be relevant.

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.

DBG use-cases:
1. Please see „HQLA“ in Germany, went live in December 2019. (Link: "https://www.hqla-x.com/")
2. Please see BLOCKBASTER for digital assets, DVP settlements on DLT (link "https://www.bundesbank.de/resource/blob/766672/29feab3f9079540441e3abda1ed2d2c1/mL/2018-10-25-blockbaster-final-report-data.pdf"
3. Please see “Digital Money” to the wholesale clients. Eg. Collateralized Coin (link "https://www.deutsche-boerse.com/dbg-en/media/press-releases/Commerzbank-Deutsche-B-rse-and-MEAG-to-reach-further-step-in-post-trade-services-using-distributed-ledger-technology--1631510")
4. Please see trusted third party for tokenization of securities, and custody of the physical asset (link: "https://www.deutsche-boerse.com/dbg-en/media/press-releases/Commerzbank-Credit-Suisse-and-UBS-execute-first-live-transactions-on-the-Deutsche-B-rse-HQLAx-securities-lending-platform-1631518")

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.

Depending on the use cases the benefits/efficiency gains are different.

DLT will enable stakeholders involved in the issuance process in achieving:
- Increased transparency
- Cost reduction
- Speed
- Resilience
- Reconciliation of processes
- Data consistency
- Full audit trail

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.

Beneficial, but depended on the rules/governance applied. If tech-neutrality is applied, then the risks should be addressed. Only the „new“ risks resulting from the technology (forks, whales, network integrity etc.) need to be mitigated.

There is a great difference between public/permissionless and private/permissioned networks with regard to associated risks. Further, there are risks associated with smart contracts, as they could transfer "legal language" into codes. This raises e.g. the question who will be responsible for the code.

Even if the DLT provides for de-centralisation, in a highly regulated environment gatekeepers and operators must be in place to safeguard the financial markets, a full outsourcing of regulatory duties to a system without clear responsibilities endangers the capital markets. Also, financial intermediaries/trusted third parties play a useful role in administrating and managing assets for investors. This could be done also by trusted third parties as gate keepers.

Considering the financial crisis, CCPs and CSDs have proven to add significant stability to the markets. Accordingly, we foresee an even more important role for CCPs and CSDs to ensure trust in such a new technology. Certainly, operations and systems may greatly benefit from DLT.

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.

Even if the DLT provides for de-centralisation, in a highly regulated environment gatekeepers and operators must be in place to safeguard the financial markets, a full outsourcing of regulatory duties to a system without clear responsibilities endangers the capital markets.

Also, financial intermediaries play a useful role in administrating and managing assets for investors. Considering the financial crisis, CCPs and CSDs have proven to add significant stability to the markets.

Accordingly, we foresee an even more important role for CCPs and CSDs to ensure trust in such a new technology. Certainly, operations and systems may greatly benefit from DLT.

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

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

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

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

We rather disagree, because we would prefer a regulatory solution for both, permissioned and permissionless systems, in order to ensure technology neutrality and to avoid fragmentation as well as different interpretation of the guidelines in the Member States.

This should include a definition of digital security assets, specified in level 2, if needed, and potential amendments to existing regulatory requirements, e.g. in order to address new technology-related risks. Given that this technology is new, a unified regulatory framework across the EU would help to effectively address risks, to provide for a reliable regulatory basis for business initiatives in this area and to build a Single Market.

If, however, the European Commission would consider taking a gradual approach, would this mean that permissionless systems would fall out of scope, which might be dangerous?

Also what means "gradual" (e.g. timing-wise, phasing, which parts in which timeline)? Could lead to an unlevel playing field with existing systems (See also Q5).

B. Assessment of legislation applying to 'security tokens'

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

The Market in Financial Instruments Directive framework consists of a directive (MiFID) and a regulation (MiFIR) and their delegated acts. MiFID II is a cornerstone of the EU's regulation of financial markets seeking to improve their competitiveness by creating a single market for investment services and activities and to ensure a high degree of harmonised protection for investors in financial instruments. In a nutshell MiFID II sets out: (i) conduct of business and organisational requirements for investment firms; (ii) authorisation requirements for regulated markets, multilateral

trading facilities, organised trading facilities and broker/dealers; (iii) regulatory reporting to avoid market abuse; (iv) trade transparency obligations for equity and non-equity financial instruments; and (v) rules on the admission of financial instruments to trading. MiFID also contains the harmonised EU rulebook on investor protection, retail distribution and investment advice.

1.1 Financial instruments

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

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

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

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

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

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

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

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

It is important to clarify that if digital-assets, like digital securities, qualify as financial instruments (according to the MiFID II definition of financial instruments in Section C of the MiFID II Directive), are already subject to existing rules.

Digital securities only become attractive for institutional investors when the associated risks are addressed in the regulatory and legal framework which builds the basis for a stable environment.

Whether digital security asset qualifies as financial instrument or not, is resulting in a fundamental difference with a view to the regulatory framework for services related to digital security (e.g. security token). In case of

qualification as financial instrument, investment services related to digital security assets (e.g. security token) will fall within the scope of MiFID II, in particular license and investor protection requirements, and of other regulation related to financial instruments, such as the MAR.

Clarity about the applicable regulatory framework is an important requirement for the development of digital security assets because it will provide for a reliable basis to assess the (regulatory) costs attached to respective business initiatives.

It is also important for investors because the level of trust they will put in digital security assets will depend on the level of investor protection requirements service providers need to observe.

We believe that digital security assets only become attractive for institutional investors when the associated risks are scalable, also in the regulatory and legal context. (See also Q5)

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.

From our point of view, there are no real best remedies, except the inclusion of “digital securities”, as a “financial instrument” defined in MiFID II under Annex I, Section C of the MiFID II (1)-(11). They should be treated as such an instrument, e.g. if the embodied value is a share, then all rules for shares apply, if the embodied value is a commodity, then all rules for commodities apply. See question 5.

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.

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.

To prevent that digital hybrid assets act as “shadow”- digital securities and therefore circumvent financial rules, the full regulatory framework should be applied to them. Regulators should foresee a review-cycle of three years to reassess the developments of digital hybrid assets

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.

Rules for investment firms should apply, but IT risks should be addressed and properly mitigated. The current regulation should reflect potential new financial services related to digital-assets. Please refer to ISO standards and the German Banking Act as a positive example.

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.

1.3 Investment services and activities

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

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

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

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

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

The key issue is which services, with a view to the purpose of MiFID II, should be subject to a license requirement and prudential requirements under MiFID II that apply to investment services currently listed in the annex to MiFID II. If new services would be added to the list, specific requirements/exemptions could be necessary.

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.

In our view, by way of transposition of MiFID II into German law no particular requirements were introduced that should be considered to specifically facilitate or prevent the use of DLT for investment services and activities.

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 line with IOSCO´s report “Issues, Risks and Regulatory Considerations in Relation to Crypto-Asset Trading Platforms”, trading venues should follow the same rules.

Even so called “decentralized exchanges” should always ensure clear responsibilities with regard to governance and the fulfillment of prudential requirements of TVs. We propose that digital-assets should be traded on trading venues exclusively as defined in MiFID, i.e. on regulated markets, MTFs or OTFs. Trading venues should be responsible for providing and ensuring equal market rules, market integrity, detecting and sanctioning mis-trades.
We promote a trading obligation for digital-/crypto-assets that qualify as financial instruments (i.e. trading on exchanges or MFTs/OTFs).

Without trading obligation, i.e. with competing trading functionalities, we would stress that such functionalities should be covered in case there is a risk of circumvention of requirements for trading venues. RfQ models could be offered by trading venues but could also be regulated brokerage business.

RfQ platforms and de-centralised exchanges should be regulated as MTFs requiring a market operator being responsible for providing for and enforcing equal market rules, maintaining market integrity, detecting and sanctioning mistrades etc.

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.

Investor protection rules are appropriate for digital securities. Potential amendments of such rules as a result of the MiFID II Review should consider specific risks attached to digital-assets.

To realise the potential of the new asset class, the usual rules should apply in general, but if necessary, additional IT related requirements shall apply (e.g. safeguarding the integrity of a DLT-network).

Potentially, extended information requirements with regard to new technology.

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.

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

5000 character(s) maximum

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

No, we do not see any particular issue by applying MiFID II, according to the principle “same business, same risk, same rules.”

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.

DBG supports European efforts to create an inclusive environment for access to finance for SMEs. For example, our “Scale” segment for small and medium-sized enterprises on the Frankfurt Stock Exchange has been registered as “SME Growth Market” since December 2019. This is a category of multilateral trading venues (MTFs) in Europe, specifically targeted at SMEs and meeting EU-wide standards. The aim is to facilitate access to capital for SMEs, to enhance the reputation of such markets and the attractiveness of capital market financing. With Scale, DBG already addresses both growth companies and traditional SMEs.

Currently over 57 stock and bond issuers are listed, financial service providers are represented as well as industrial or software companies. Scale creates additional transparency through research reports and regular issuer roadshows in Europe.

Therefore, we agree with the aims of the EC´s latest communication “An SME Strategy for a sustainable and digital Europe”, published on 10 March. It is possible that blockchain-based initiatives may enable the issuance and trading of SME securities across Europe.
However, trading on blockchain-based initiatives should comply with all regulation mentioned. Currently, some of these systems are not only considered slower than existing current systems (lower latency), but have also the problems of price transparency/arbitrage. As of now, we think that many questions have to be solved in using DLT for trading in secondary markets, regardless of the size of the companies right now.

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.

Resilience measures are important and regulators should always ensure clear responsibilities.

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.

Admission to trading should only be allowed by trading venues (i.e. regulated markets, MTFs or OTFs), based on their rules and regulations, and should follow the same regulatory framework as today.

However, allowing crypto-currencies to trading may shift the responsibility from an issuer to the operator (as no issuer exists), also with regard to the monitoring of technical issues (like "forks").

Also, physical settlement would require relevant regulated settlement systems being in place.

Further, we would like to refer to Art. 3 CSDR and the obligation to organise the settlement of transactions in crypto securities concluded at a trading venue via a Central Securities Depository.

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.

Today, only financial intermediaries are allowed to have access to trading venues. The current regulation does not allow for access to trading venues to a broader base of clients.
Exchanges and MTFs can admit to trading only entities that are engaged in trading on own account or on behalf of customers whereas such limitations do no apply for bilateral trading models, such as RfQ-models, that are regulated as brokerage business.

The admission for third-country participants should also follow the current MiFID II regime (until there is a MiFID II equivalence decision taken, national regimes apply for third-country firm access to European trading venues).

1.10 Pre and post-transparency requirements

In its Articles 3 to 11, MiFIR sets out transparency requirements for trading venues in relations to both equity and non-equity instruments. In a nutshell for equity instruments, it establishes pre-trade transparency requirements with certain waivers subject to restrictions (i.e. double volume cap) as well as post-trade transparency requirements with authorised deferred publication. Similar structure is replicated for non-equity instruments. These provisions would apply to security tokens. The availability of data could perhaps be an issue for best 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.

As we have pleaded above, digital security assets should be integrated in the MiFID II definition of financial instruments.

It is vital that the MiFIR requirements on transparency for trading venues (both for equity and non-equity instruments) apply in the same way for digital-assets as they currently apply for any other financial

instrument. Therefore, digital securities need to be able to report the number of details identifying the financial instrument that are required for a reporting through an Approved Publication Arrangement (APA), e. g. the identifier of the financial instrument; the price, volume and the time of the transaction or the code for the trading venue.

This information ensures the integrity of markets, mandating national competent authorities (NCAs) and ESMA to ensure integrity by monitoring investment firms' activities as to their honest, fair and professional market behavior. In order to detect and investigate on potential market abuse, any transactions of a reportable financial instrument – including digital security assets – need to be covered by the transaction reporting requirements to safeguard the integrity of the financial market.

Transparency in the financial market is key. The Financial Crisis of 2008 which started in the non-transparent Credit Derivatives Markets has shown that a lack of transparency in the Capital Market affected the financial stability as a whole. An APA promotes transparency in the financial markets which strengthens financial stability. In addition to the validation, enrichment and publication of the transmitted data, an APA undertakes the data-intensive and complex calculation of regulatory delays in data publication (deferrals) and is therefore beneficial for regulators and financial institutions.

We believe that pre- and post-transparency provided via an APA and through transaction reporting by investment firms (or via an ARM) plays a key role for the stability of the financial market. Trades and transactions in digital securities shall be reported via an APA in order to maintain the achievements we attained so far in regard to financial stability

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.

As addressed in question 74, we believe that the MiFIR requirements on transparency for trading venues need to apply for digital security assets in the same way as they currently apply for any other financial instrument. Digital security assets are fully capable to provide the data that is need for reporting. Therefore, we do not see any issues which could prevent applying the MiFIR requirements on transparency for security tokens.

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 line with our answer to question 74, we strongly recommend that the current MiFIR requirements on transaction reporting need to apply for digital securities as they apply for any other financial instrument. MiFIR provides an extensive and complex set of transaction reporting details such as e.g. branch reporting flags, a Legal Entity Identifier (LEI) for legal entities eligible for a LEI, the Trader ID, the Algo ID or OTC post-trade flags.

These information ensure the integrity of markets, mandating national competent authorities (NCAs) and ESMA to enforce this integrity by monitoring investment firms' activities as to their honest, fair and professional market behavior. In order to detect and investigate on potential market abuse, any transactions with a reportable financial instrument – including security tokens – needs to be covered by the transaction reporting requirements. Any exceptions in this regard need to be excluded as this could endanger the integrity of the financial market.

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.

Basically, we consider the definition of insider dealing pursuant to Art. 8 MAR, including the acquisition and disposal of security token (to be qualified as financial instruments) as well as the cancelation or amendment or respective orders, to be sufficient.

However, it should be assessed whether with a view to the IT environment for trading of digital securities the definition should be further specified or even broadened in order to avoids any loopholes. Supervisory bodies may have to adapt.

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.

Also the definition of markets manipulation seems to be sufficiently broad, in particular as it covers, besides disseminating and transmitting of information, not only entering into a transaction or placing of orders but any other activity or behavior. We see the need to take into account the IT environment for trading of digital securities and to assess whether a specification or amendment of the definition should be considered.

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.

We would propose to apply for digital crypto-currencies also the MAR rules. If digital-assets, which are currently not covered by the current definitions of financial instruments (e.g. crypto-currencies) would be integrated in the MiFID II definition of financial instruments [new category (12)], also MAR would be applicable. (See Q5)

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	2	3	4	5	Don't know / no opinion /

	(not a concern)				(strong concern)	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.

No DBG response.

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.

No DBG response.

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.

No DBG response

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.

If there is an obligation to publish a prospectus for a digital security all existing rules and exemptions should apply. Depending (e.g.) on the size of the digital security asset issuance, the targeted investor group, the underlying type of the security, there are existing rules and exemptions today, which should apply and should be enough. Additional exemptions could be established later, if the need in the market arises.
Additionally, it might be useful to inform in the prospectus about the technological features of the assets, especially if a smart contract is included. See for example BaFin`s Prospectuses Guidance Notice (link: "https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_wa_merkblatt_ICOs_en.html") on prospectus and authorisation requirements in connection with the issuance of crypto-tokens.
Ideally information should be explained in an "understandable" manner to reduce complexity and the length of the prospectus and inherent costs.

As the technology is new and additional features arise, investors need more information on the following aspects: If applicable, which type of chain is used (public vs private / permissioned vs permissionless)? Which type of smart contract is used? Which type of safety and resilience measures are applied in the used smart contracts (e.g. technical malfunction detection tools) Which type of token governance mechanism is included? Which types of risks are addressed with regard to technological, economical or environmental? It could be beneficial to aggregate this information into a rating for investors about the asset in question, provided by a trusted third party.

4.2. The drawing up of the prospectus

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

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

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

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

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

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

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

5000 character(s) maximum

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

Yes, see also Q82
In Germany, the task of approving the prospectus has been transferred to BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht). This applies both to prospectuses for public offerings and to the prospectuses for admission to trading on the stock exchange. The Frankfurt Stock Exchange or Deutsche Börse AG have no influence on the content of these prospectuses. Against this background, we refer to the competent authorities in Germany. However, we consider it appropriate to grant exceptions to the basic requirement of a prospectus, provided that it is legally and factually appropriate

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.

As digital securities are securities, they must be able to be identified via an ISIN. This would also help to process digital securities in established IT systems. To our knowledge, some numbering agents have confirmed that they have started allocated ISINs to tokens (mostly securities tokens). Beyond ISIN (relevant for security tokens, and possibly hybrid tokens), some other existing global identifiers could also be leveraged, for instance the ISO 4217 currency code could very well be leveraged for crypto-currencies, providing similar benefits to the market than the ones referred so far for securities. We generally promote the adoption of established ISO standards for the identification of digital-assets, while recognising that we will likely need a separate, additional digital-asset identifier, at least for those assets that are neither securities nor currencies (to our knowledge, work in progress within ISO reg. “digital token identifier”).

For example, a possible identifier for crypto-currencies is debated at the level of ANNA (international ISO registration authority). Furthermore, with regard to reporting obligations of digital security assets, prudential reporting requirements could be considered.
At the level of ANNA (the ISO registration authority for the ISIN standard), some numbering agents have confirmed they have started allocated ISINs to digital-assets (mostly securities tokens). But overall the picture remains blurred, also because there is still uncertainty as to how these tokens must be treated legally speaking (need to be considered as financial instruments). The reality is, that very few countries have reached that level of clarity/maturity in their national legislation so far. The topic is being discussed between numbering agents within the ANNA Task Force 22, of which Deutsche Börse Group is a member.

The matter is also being discussed within ISO in the context of a possible new standard (Digital-asset Identifier) for which a dedicated working group has been created. A working draft is currently at voting stage within ISO.

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.

As the technology is new and additional features/difficulties arise, investors need more information on the following aspects:

- If applicable, which type of chain is used (public vs private / permissioned vs permissionless)?
- Which type of smart contract is used?
- Which type of safety and resilience measures are applied in the used smart contracts (e.g. technical malfunction detection tools)
- Which type of token governance mechanism is included?
- Which types of risks are addressed with regard to technological, economical or environmental?

It could be beneficial to aggregate this information into a rating for investors about the asset in question, provided by a trusted third party.

Ideally and as a general remark, a prospectus should be “understandable” for investors. Those information should be summarized in an “understandable” manner to reduce the complexity and the length of the prospectus and costs.

Also, there is the question regarding the application of prospectus rules to public blockchains and the circumvention of those obligations. In our view, ideally, there should be someone identified to be responsible for providing the prospect to competent authorities.

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.

See also above: If there is an obligation to publish a prospectus for a digital security asset, we think that all existing rules and exemptions should apply.

If necessary, a new simplified regime could be introduced in the future, however this should still include the technical details.

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

- ◉ Completely agree
- ○ Rather agree
- ○ Neutral
- ○ Rather disagree
- ○ Completely disagree
- ○

Don’t know / no opinion / not relevant

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

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

Yes.

Furthermore, from our point of view it is necessary to inform about DLT specific risks, for example on the functioning of the algorithm for the used smart contract, the specifics what feature are programmed (and which are not).

Meanwhile, the operator of a private blockchain could monitor the quality of the security token and their features.

The prospectus should also inform about those incidents and responsibilities (e.g. related to corporate actions), which are not programmed in the smart contracts. This also relates to the question of changes to / failures of the algorithm of smart contracts already in the market

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.

To ensure market integrity, any service provider offering CSD-like services (core services pursuant to Section A of the annex to CSDR, i.e. notary service, central maintenance and settlement services) should

comply with the CSDR and SFD, regardless of the used technology.

To allow institutional investors to benefit from the technological advantages of digital-assets, those assets need to fulfill the necessary requirements regarding governance standards (which are e.g. a record of the existence of a security and a conformation about the total amount securities issued). This also ensures investor protection.

CSDR does not prescribe any technical execution method for the registration of securities. At the same time, the notion of a 'securities account' is defined in CSDR in a broad way, i.e. "an account on which securities can be credited or debited". Notwithstanding, it would be beneficial to receive guidance from ideally ESMA regarding the application of this framework by CSDs to the digital-asset environment, as it was already done in some countries, e.g. France.

On a private blockchain run by a CSD, relevant records could be qualified as securities accounts. However, all digital-assets would need to qualify as securities.
The transfer of ownership with respect to such dematerialized securities through the entire custody-chain would need to be harmonized in the Member States (e.g. occurring upon agreement and booking in an adequate CSD or custodian system). Only then, legal certainty with respect to a relevant discharge of obligations can be achieved.
We would welcome any form of cash on ledger solution/ digital money.

The transfer of ownership with respect to such dematerialized securities would need to be harmonized in the Member States, e.g. occurring upon agreement and booking in an adequate CSD or custodian system. Only then, legal certainty with respect to a relevant discharge of obligations may be achieved.

"Form follows function": Today CSDs perform important functions linked to the initial issuance and further distribution of securities on behalf of an issuer. Also, they operate a SSS and fulfill therefore at least one of the following two core services to the market: notary and central maintenance services including settlement and safekeeping services (Art 2 CSDR). These functions are important for market integrity. One of the key critical functions that a CSD is required to fulfil is the so-called "notary function", it involves the initial recording of the existence of a security and equally importantly the confirmation of the total issued amount of a given instrument and the confirmation by an issuer CSD that the total amount of securities held by all participants in the CSD equals the total amount of securities issued.

Therefore, any service provider offering these services and functions should comply with the CSDR and SFD, independent of the used technology.

Today, there exist assets, which do not have to be registered by a CSD. Usually, they only have small volumes and liquidity. Institutional investors are often not allowed to invest in this kind of assets, due to their internal governance rules. To allow institutional investors to participate from the technological benefits of digital-assets, those assets need fulfill the necessary required governance standards (which are e.g. a record of the existence of a security and a conformation about the total amount securities issued). This also ensures investor protection.

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.

When using custody chains in an DLT environment, the relevant rules on holding and title transfer need to be applicable and clear, i.e. if a CSD uses DLT, custodian bank 1 uses legacy, sub-custodian 2 uses DLT (etc.) the booking in the last custody system for the benefit of the end-customer should be constituent.

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.

Please see Q88.

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.

In absence of a law on dematerialised securities (and covering all relevant securities) in Germany, the existence, custody and transfer of ownership of digital-/crypto-assets, specifically security tokens, is unclear causing significant legal uncertainty. However, this topic is expected to be addressed in the near future by the German government.

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.

We do not have any concerns in this regard.

91.2 Please explain your reasoning for your answer to question 91:

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

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

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

See question 90 with regard to "dematerialisation".

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.

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.

The definition of “system” is sufficiently flexible as it covers contractual arrangements and not technical systems. Current provisions of SFD already cater for some activity in the domain of digital- assets, however, attention shall be given in a future review to aspects such as their explicit inclusion in the definition of “transfer orders”. However, the definition of “transfer order” would need to cover all relevant digital-assets including crypto-currencies to cater for finality of relevant instructions.

A system operator must be responsible for the relevant “systems” and “transfer orders”. Consequently, with regard to DLT-solutions, those with private permissioned blockchain are most viable, even if public permissioned solutions are also conceivable. Regulators should ensure that requirements of CSDR and SFD are not circumvented by DLT.

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.

Please see question 93.

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.

Please see question 93.

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

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

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

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

7. Financial Collateral Directive (FCD)

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

						Don't know /

	1 (not a concern)	2	3	4	5 (strong concern)	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.

No DBG response.

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.

No DBG response.

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.

No DBG response.

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.

No DBG response.

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

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

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

5000 character(s) maximum

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

8. European Markets Infrastructure Regulation (EMIR)

The European Markets Infrastructure Regulation (EMIR) applies to the central clearing, reporting and risk mitigation of over-the-counter (OTC) derivatives, the clearing obligation for certain OTC derivatives, the central clearing by central counterparties (CCPs) of contracts traded on financial markets (including bonds, shares, OTC derivatives, Exchange-Traded Derivatives, repos and securities lending transactions) and services and activities of CCPs and trade repositories (TRs).

The central clearing obligation of EMIR concerns only certain OTC derivatives. MiFIR extends the clearing obligation by CCPs to regulated markets for exchange-traded derivatives. At this stage, however, the Commission services does not have knowledge of any project of securities token that could enter into those categories.

A recent development has also been the emergence of derivatives with crypto-assets as underlying.

Question 101. Do you think that security tokens are suitable for central clearing?

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

101.1 Please explain your reasoning for your answer to question 101:

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

In particular digital security assets representing financial instruments are suitable for clearing as the clearing house would diminish any counterparty risk, provide for netting efficiencies (avoiding the necessity for instant settlement) and ensure physical settlement.
Risk Management services of CCPs will still be required in the future, as the financial crisis 2008 has proven. The G20 declaration of Pittsburgh strengthened the importance of CCPs in this context.

Other important functions of CCPs including multilateral netting and netting between different asset-classes, collateral and default management processes cannot be directly replaced by DLT today.

We believe that digital securities are appropriate for central clearing, therefore CCPs should be allowed to clear them in accordance with EMIR.

Further clarity is needed regarding the conditions / prudential requirements with which CCPs are allowed to clear digital-assets / derivatives with an digital-asset underlying. They should also qualify as eligible margins

In general, we believe that the relevant regulations are agnostic to the kind of systems that may be used by a CCP/ trade repositories. However, it would need to be clarified that a CCP may accept and hold digital security and payment assets for settlement and margining purposes.

The possibility of „T-instant" is no unique feature to DLT. However, as of now there seems to be a majority of participants in the market preferring T+2 due to e.g. liquidity management reasons. Also, risks with regard to insolvency and (physical) delivery are still relevant.

Using DLT would allow to segregate accounts and margin custody. This should be allowed by regulation.

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

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

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

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

5000 character(s) maximum

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

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

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

No, as stated above, transfer of ownership and finality would need to be clearly provided for by applicable law.

Please see Q101.

Settlement finality rules should be in line with the system finality using a DLT. Using DLT, segregated accounts and margin custodized should be enabled by relevant regulation.

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.

In general, we believe that the relevant regulations are agnostic to the kind of systems that may be used by a CCP/Trade Repositories. However, it would need to be clarified that a CCP may accept and hold security and payment tokens for settlement and margining purposes. (e.g. digital-/crypto-assets should also qualify for eligible margin assets).

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.

Please see Q101.

9. The Alternative Investment Fund Directive

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

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

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

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

	1 (not suited)	2	3	4	5 (very suited)	Don't know / no opinion / very suited
AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;	○	○	○	○	○	◉
AIFMD provisions requiring AIFMs to maintain and operate effective organisational and administrative arrangements, including with respect to identifying, managing and monitoring the conflicts of interest;	○	○	○	○	○	◉
Employing liquidity management systems to monitor the liquidity risk of the AIF, conducting stress tests, under normal and exceptional liquidity conditions, and ensuring that the liquidity profile and the redemption policy are consistent;	○	○	○	○	○	◉

AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets;	○	○	○	○	○	◉
Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments.	○	○	○	○	○	◉

105.1 Is there any other area in which the provisions of the EU AIFMD legal framework are appropriately suited for the effective functioning of DLT solutions and the use of security tokens? Please specify which one(s) and explain your reasoning:

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

No DBG response.

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.

No DBG response.

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

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

106.2 Please explain your reasoning for your answer to question 106:

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

No DBG response.

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.

No DBG response.

107.2 Please explain your reasoning for your answer to question 107:

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

11. Other final comments and questions as regards tokens

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

Question 108. Do you think that the EU legislation should provide for more regulatory flexibility for stakeholders to develop trading and post-trading

solutions using for example permissionless blockchain and decentralised platforms?

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

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

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

No, we believe that existing regulation on the financial markets have proven to ensure market integrity. Those rules should be followed, and foreseen functions of service providers ensured, regardless of the technology used (e.g. public permissionless systems).

Role of FMIs: Technology is an enabler to perform services, i.e. DLT could be seen as an evolution for the financial industry.

FMIs (such as exchanges/MTFs, CCPs and CSDs) today provide important functions to markets as proven in and after the financial crisis and will continue to do so in the future.
FMIs should be explicitly allowed to handle all forms of digital-assets.

Even if their roles might change, their core functions will still be needed to ensure trust in markets in a “new” digital or DLT environment and cannot be all performed exclusively by the new technology.

A trusted third party is always needed in the financial industry to create trust in the market; also it holds high responsibility, especially to address following functions such as: 1) Control access/admission 2) Set rules for the participating nodes 3) Address potential conflicts of interest and KYC and AML requirements 4) Apply risk management 5) Be reliable for market integrity, security and other regulatory requirements.

Further, with regard to the use of decentralized platforms, which use the "proof of work"-concept, energy consumption is relative high.

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.

We see the risk of shifting responsibilities in operating financial markets to systems/platforms which in case of malfunctioning or abuse may deteriorate trust in the financial markets.

Same business, same risks, same rules: Current regulation should apply, as it has been established to ensure market integrity as a key learning from the financial crisis.

Further, only with legal certainty, market actors can develop uses cases, services and invest into innovation.

Tech-neutrality: It has to be ensured that the principle of tech-neutrality within the regulatory framework is upheld.

Regulators should ensure that requirements of regulation are not circumvented by digital infrastructures / DLT.

As long as the operator is compliant with the rules, in general, the used IT-system should not be a matter of high importance. However, technology-related „new“ risks should be taken into account.

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.

We think that the principles "same business, same risk and rules" should apply to uphold the benefits, such as market integrity or cost efficiencies.

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.

With a focus on public blockchain, we have seen fraud, misbehaviour, deteriorating the trust in these assets (e.g. ponzi schemes as with ICO/STOs in the past). We would like to stress the importance of established rules and best practices in the markets, e.g. the role of regulated financial market intermediaries to ensure transparency for investors and ensure the functioning and integrity of trading and financial transactions.

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.

Yes, see above „dematerialisation" in Germany

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.

As the EMD2 was written before the "phenomenon" of "digital money" came up. Therefore, a first classification and definition of terms of "digital payment assets", i.e. "e-money" versus "digital money" should be integrated into the directives (See Q7/Q8/Q31 etc) and the rules ideally be adjusted, where necessary.

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.

No DBG response

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.

No DBG response

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.

No DBG response

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.

No DBG response

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.

No DBG response

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