Bundesministerium Finanzen

ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

OESTERREICHISCHE NATIONALBANK EUROSYSTEM

Europäische Kommission
Generaldirektion Finanzstabilität,
Finanzdienstleistungen und Kapitalmarktunion

SPA 2 – Pavillon Rue de Spa 2 / Spastraat 2
1010 Wien
Belgium

Via E-Mail an: fisma-crypto-assets@ec.europa.eu

BEREICH Integrierte Aufsicht
GZ FMA-LE0001.230/0003-INT/2020
(bitte immer anführen!)

SACHBEARBEITER/IN Mag. Philip Gollmann
TELEFON (+43-1) 249 59 -4213
TELEFAX (+43-1) 249 59 -4299
E-MAIL philip.gollmann@fma.gv.at
E-ZUSTELLUNG: ERsB-ORDNUNGSNR. 9110020375710

WIEN, AM 19.03.2020

EK-Konsultation: EU-Rechtsrahmen für Kryptoanlagen

Sehr geehrte Damen und Herren,

bezugnehmend auf die öffentliche Konsultation der Europäischen Kommission zu

„*Finanzdienstleistungen – EU-Rechtsrahmen für Kryptoanlagen*"

erlauben wir uns Ihnen anbei die gemeinsame Stellungnahme des österreichischen **Bundesministeriums für Finanzen (BMF)**, der **Österreichischen Nationalbank (OeNB)** und der **Österreichischen Finanzmarktaufsichtsbehörde (FMA)** zukommen zu lassen.

Selbige Stellungnahme wird zur leichteren Auswertung ebenso im Rahmen des Online-Fragebogens zur gegenständlichen Konsultation (siehe: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12089-Directive-regulation-establishing-a-European-framework-for-markets-in-crypto-assets/public-consultation) eingebracht.

Wir ersuchen höflich um Berücksichtigung unserer Anregungen und stehen für Rückfragen gerne zur Verfügung.

Finanzmarktaufsichtsbehörde
Bereich Integrierte Aufsicht

Für den Vorstand

MMag.a Dr.in Julia Lemonia Raptis, LLM LLM

Dr. Christoph Seggermann

elektronisch gefertigt

Signaturwert	UrPF1hG4OvmawbfrBZpXjUWthzdquF/IdPyx8JnwgsozXVFS7X79hj4J9yJHzzch+bQ3TrMHVc23QFnvYNnd qarYDLl0cFQkxgwKtNj3XWsiAfU1nfUVa7OLqa+MFEj1PP1Mhh5s2Hn6jGuf7Fa/QAD7Yn9hT9m4/7Sowolf kKB1mrXFGMqnHh5l9eTB5vqbOzt3me/s/T2rIg15fv7uUcdYOJaU6a9Byx5M+H0JMG3toyIw8n1pEmCYFsW1 6YO1tYrkyBRopoP/I+chvbEWzQjK6jk2S4woFBPOjNfFXrVXuIVp4SgbHRnW0JV539gJijssB+gp+5ivmUZf ubR+Jw==	
	Unterzeichner	Österreichische Finanzmarktaufsichtsbehörde
	Datum/Zeit-UTC	2020-03-19T19:44:05Z
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	532114608
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

EUROPEAN COMMISSION
Directorate-General for Financial Stability, Financial Services and Capital Markets Union

CONSULTATION DOCUMENT

On an EU framework for markets in crypto-assets

Disclaimer

This document is a working document of the Commission services for consultation and does not prejudge the final decision that the Commission may take.

The views reflected on this consultation paper provide an identification on the approach the Commission services may take but do not constitute a final policy position or a formal proposal by the European Commission.

You are invited to reply by **19 March 2020** at the latest to the online questionnaire available on the following webpage:

https://ec.europa.eu/info/publications/finance-consultations-2019-crypto-assets en

Please note that in order to ensure a fair and transparent consultation process **only responses received through the online questionnaire will be taken into account and included in the report summarising the responses.**

This consultation follows the normal rules of the European Commission for public consultations. Responses will be published unless respondents indicate otherwise in the online questionnaire.

Responses authorised for publication will be published on the following webpage:

https://ec.europa.eu/info/publications/finance-consultations-2019-crypto-assets_en"

INTRODUCTION:

1. 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 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 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

[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

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[10] - MiFID II - or as electronic money/e-money under the Electronic Money Directive - EMD2[11], 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.

---

[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] Market in Financial Instruments Directive (2014/65/EU)

[11] Electronic Money Directive (2009/110/EC)

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"*[12]. 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"*[13].

2. Responding to this consultation and follow up to the consultation

In this context and in line with Better Regulation principles[14], 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**[15]. **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 cryptoassets 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**

[12] Mission letter of President-elect Von der Leyen to Vice-President Dombrovskis, 10 September 2019
[13] Joint Statement of the European Commission and Council on 'stablecoins', 5 December 2019
[14] European Commission, 'Better Regulation: Why and How'
[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).

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[16], MIFID II, the Central Securities Depositaries Regulation[17]...) 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.**

PUBLIC CONSULTATION

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.

1) **Have you ever held crypto-assets?**
   - **Yes**
   - **No**

2) **If you held crypto-assets, what was your experience?** [Insert text box]

2.1. Was it simple and straightforward to buy them?
- **simple**
- **neither easy nor hard**
- **complex**

2.2. Did you feel sufficiently well informed about your rights, the risks and opportunities?
- **Yes**
- **No**

2.3. Did you buy the crypto-assets from an EU or non-EU vendor, exchange or trading platform?
- **EU**
- **Non-EU**
- **Don't know**

2.4. Did you hold the crypto-assets with a custodial wallet provider?

[16] Prospectus Regulation (2017/1129/EU)
[17] Central Securities Depositaries Regulation (909/2014/EU)

- **Yes**
- **No**

2.5. What type of crypto-assets, have you held?

- **Crypto-assets backed by assets (such as cash, gold, shares, bonds, or other real world assets...)**
- **Payment tokens/virtual currencies (such as bitcoin)**
- **Crypto-assets giving the right to use a service or access a product**
- **Other**

2.6. Did you make any profit or a loss on the crypto-assets you held?

- **Profit**
- **Loss**
- **I was able to use them for the services or products promised**
- **Other**

2.7. Have you experienced any loss as a result of safekeeping issues with your crypto-assets?

- **Yes**
- **No**

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

- **Yes**
- **No**
- **Don't know/no opinion**

Please explain the reasons why you are planning to hold crypto-assets (if needed).
[Insert text box]

4) If yes, in what timeframe?

- **in the coming year**
- **2-3 years**
- **more than 3 years**

II. Classification of crypto-assets[18]

There is not a single widely agreed definition of 'crypto-asset'. In this public consultation, a crypto-asset is considered as *"a digital asset that may depend on cryptography and exists on a distributed ledger".* This notion is therefore narrower than the notion of *'digital asset'*[19] 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

[18] 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.

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

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.

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**~~

   Please explain your reasoning (if needed). [Insert text box]

Crypto-assets often fulfil a similar purpose as financial products, representing financial claims, means of payments, etc. In this context crypto-asset service provider and intermediaries fulfil similar roles and are prone to similar risks as financial services providers. On the other hand the wider term digital asset does cover digital representations of other assets which are not similar to financial products, therefore applying a supervisory regime designed for crypto-assets similar to financial products would be overburdening and disproportionate. From a technology's perspective literally everything can be digitalized, from identity characteristics to goods and services (note: digitalisation of goods and services has been common for decades due to businesses issuing digital vouchers). The specific risks attached to financial products require a stricter regulatory approach, which is inadequate for other types of assets. Including digital assets in general in a new European supervisory framework solely because a specific technology is used (DLT) seems unnecessary.

Therefore the scope should be limited to crypto assets.

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**~~

If yes, please indicate the best way to achieve this classification (non-legislative guidance, regulatory classification, a combination of both...). Please explain your reasoning. [Insert text box]

Legal certainty and a level playing field are key. The best way to implement classification depends on the desired legislative approach. If the goal is to only adapt existing European legislation to crypto-assets (e.g. prospectus regulation, e-money directive), then a legally binding classification is not essential, because crypto-assets could be subsumed under existing legal terminology (e.g. e-money). In this case, the focus should be non-legislative guidance or, if need be, adaption of existing legislation to make it compatible with crypto-asset applications. If the Commission's intend is to create a holistic regulatory framework for the entire crypto-economy (addressing currently regulated and unregulated crypto-assets), then a legal definition and classification would be needed to properly regulate different types of crypto-assets. Such a regulatory framework should be innovation-oriented, risk-based and proportionate.

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).** [Insert text box]

There is no legal binding classification in Austria, but the current practice commonly refers to the classification in payment, security and utility tokens (https://www.fma.gv.at/en/cross-sectoral-topics/fintech-navigator/initial-coin-offerings/). However, under existing law this is more a crutch for comprehension and communication purposes than a tool for definition. What matters are the legal terms (wheter or not the crypto-asset falls under the terms “financial instrument”, “security”, “e-money”, “payment instrument”, etc.). The FMA has cases in which lawyers refer to one of the classes, but the functionality of the token is broader, hybrid or indicates another class – this is usually the case for self-determined utility tokens that in fact are used as payment tokens with one or more providers, or as investment in the company. Therefore, the terminology used by market participants needs to be assessed under the applicable national and European legal terminology on a case-by-case basis.

Some international committees like International Token Standartization Association (ITSA) or the US Crypto Rating Council (CRC) already have first experiences in classifying crypto assets. Both take a slightly different approach: ITSA applies the common trisection (payment, security, utility), whereas the CRC works with a probabilistic scale of 1 to 5 to qualify a token as a security. Because more than a demarcation of security tokens is needed, and because a probabilistic classification leaves a lot of uncertainty, the trisection of ITSA and the existing market usage is more meaningful, however by far not optimal for supervisors (please see our suggestion under point b below).

a) A classification along the lines of different functionality is already common and reasonable, because it emphasizes the different purpose and usage of instruments:

A *payment crypto asset* would be an asset that is used as a means of payment. This means its purpose is that third parties accept it with debt-discharging effect, no matter the contractual basis between the parties. The definition should not say that a payment crypto asset *is issued as* a means of payment because this would exclude most of the decentrally generated crypto assets like Bitcoin that have no issuer.

An *investment/security crypto asset* would be an asset that has the same features as a transferable security according to MiFID II and Prospectus Regulation (i.e. embodiment of a financial asset, negotiability on capital markets, comparability to shares, bonds or similar securities, see MiFID II Section C of Annex I).

A *utility crypto asset* would be an asset that embodies no future payment claims but the delivery of goods or services;

However, the trisection of payment, security and utility token also poses the risk that these terms are being confused with existing instruments which are similarly named (e.g. payment token vs payment instrument/ means of payment/ e-money; security token/investment token vs. transferable security/ financial instrument). Furthermore, a trisection does not account for hybrid forms and no-right-tokens, which are of high practical relevance and would still need a case-by-case-assessment which would require further criteria. Generally, the trisection definition seems to be mainly suited for communication purposes and easy understanding but offers little when defining a regulatory scope.

b) An alternative approach would be the stipulation of a *single crypto-asset-class* (cross-class-definition of crypto-assets) and regulate specific activities linked to this cross-class-definition of crypto-assets.

This regulatory approach is similar to the regulatory technique used in the 5. AMLD. In general, there can be benefits in a horizontal regulatory approach to ensure consistency, legal clarity as well as a minimum level of consumer protection and to avoid regulatory arbitrage.

A crypto-asset service provider could fall within the proposed regulatory scope if **specific** legally stipulated **services** in regards to **regulated crypto-assets** (as defined in the cross-class-definition) are offered. These regulated services could include the public offering of, trading on market places (exchanges) for and custody services for crypto assets and would be subject to regulatory requirements (e.g. fit-and-proper / minimum capital / risk management). However, it is important to achieve a well-balanced and proportionate regulatory framework and impede over-regulation.

The scope of a single crypto-asset-class approach should be proportionate and cover only token which offer the following features:

- Standardization
- transferability
- purpose of being traded on capital markets
- embodiment of a financial claim (this captures token with investment function and includes token which offer for instance a payback if a pre-purchased utility is not created, to capture pre-sales of products that are more an investment in the company)
- *and/or* usage for payments at third parties (this captures token with payment function)
    - whereas limited networks could be exempted, similarly to the PSD II and the EMD 2.

A broad and cross-class-definition of crypto-asset could mitigate the issue of hybrid token as well as token that change their functionality through their life cycle as this happens reguarly in the early phase of crypto-assets. Experience shows that both types of token regularly defy classification as a specific asset type. A cross-class definition could cover classic payment / investment / utility token as well as outliers.

If crypto-assets are within the scope of existing regulatory frameworks (e.g. Prospectus Regulation, MiFID II, EMD 2, PSD 2), then those rules should apply. This would mean for instance that payment token which are classified as e-money would follow the rules for e-money laid down in the EMD 2. On the other hand, payment token which are not classified as e-money but fall within the broader scope of the term “regulated crypto asset” (e.g. Bitcoin) would only follow the general rules for regulated crypto-assets.

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**~~

   Please explain your reasoning (if needed). If yes, indicate if any further sub-classification would be necessary. [Insert text box]

A distinct category for „hybrid tokens" would offer little benefit. On the other hand it could even increase the legal uncertainty due to the fact that hybrid tokens are not a distinct category of crypto-assets but a blend of tokens with payment / investment / utility character. In contrast to creating a distinct category for hybrid token, it seems more reasonable to lay down consequences for a token that is not 100% classifiable due to overlapping characteristics. E.g. force a subsumption into one class on basis of the predominant feature, or otherwise apply the requirements for all classes in question. This could be done by guidance (e.g. recitals) or conflict-of-law rules and does not necessarily need a distinct legal category for hybrid token.

Furthermore tokens are minted which offer neither payment, investment nor utility characteristics. Although these crypto-assets offer no intrinsic business case, they are still been speculated on (e.g. "Dogecoin").

Another approach would be a cross-class-definition of crypto-assets as proposed in question 7.

The Deposit Guarantee Scheme Directive[20] (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.

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?** [Insert text box]

The Ministry of Finance, the FMA and the OeNB are currently unaware of any crypto assets, that could be qualified as deposits as per the definition in Article 2(3) DGSD.

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

[20] Deposit Guarantee Schemes Directive (2014/49/EU)

by crypto-assets that currently fall outside the scope of EU financial services legislation[21] (**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-asset sector (**C.**).

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.

10) In your opinion, what is the importance of each of the potential benefits related to crypto-assets listed below? Please rate each proposal from 1 to 5, 1 standing for "not important at all" and 5 for "very important". [insert text box]

	1	2	3	4	5	No opinion
Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs						x
Issuance of utility tokens as an alternative funding source for start-ups						x
Cheap, fast and swift payment instrument						x
Enhanced financial inclusion						X
Crypto-assets as a new investment opportunity for investors						x
Improved transparency and traceability of transactions						x
Enhanced innovation and competition						x
Improved liquidity and tradability of tokenised 'assets'						x
Enhanced operational resilience (including cyber resilience)						x
Security and management of personal data						x
Possibility of using tokenisation to coordinate social innovation or decentralised governance						x
Other						x

[21] 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 justify your reasoning (if needed). [Insert text box]

As an authority and as Ministry that do not use crypto assets itself we don't see our role in determining benefits. Benefits of using tokenisation to decentralize governance would still have to be evaluated diligently, it seems too early to judge on first projects that states and authorities are experimenting with.

From a national bank's perspective and with regards to "enhanced financial inclusion", the positive effects of crypto assets on financial inclusion depend very much on the concerned financial markets and their functional capabilities. In the EU, the financial inclusion is already on a high level due to existing legal frameworks, such as the directive on payment accounts, which gives EU citizens the right to a basic payment account. In other regions where banking systems may be less efficient, crypto assets are said to support the idea of banking the unbanked.

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[22]. Certain features of cryptoassets (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[23]. 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[24], this might change in the future.

11) **In your opinion, what are the most important risks related to crypto-assets? Please rate each proposal from 1 to 5, 1 standing for "not important at all" and 5 for "very important".** [insert text box]

	1	2	3	4	5	No opinion
Fraudulent activities					x	
Market integrity (e.g. price, volume manipulation...)					x	
Investor/consumer protection					x	
Anti-money laundering and CFT issues					x	
Data protection issues					x	
Competition issues					x	
Cyber security and operational risks					x	
Taxation issues					x	
Energy consumption entailed in crypto-asset activities			x			
Financial stability			x			
Monetary sovereignty/monetary policy transmission			x			
Other						x

[22] ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019

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

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

Please justify your reasoning (if needed). [Insert text box]

We agree with the assessment of the ECB that the primary risks with crypto-assets relate to ML/TF and consumer protection. The ECB sees no immediate threat to financial stability. However, this is just a snapshot of the current markets. We consider risks in financial stability and monetary policy not negligible but depending on further developments. For instance, elements of systemic cyber incidents can be intertwined with Financial Stability (eg: hacks on wallets on grand scale) but because of a still relatively low level of adoption of crypto-assets we do not see an imminent danger for that. However, mass-market entries of BigTech stablecoins like Facebook's Libra could change that.

Currently fraudulent activities and consumer protection issues are a common problem. Consumer complaints are regularly brought to the attention of supervisory and criminal authorities in Austria. Moreover there are obvious market integrity risks in the context of exchanges due to complex business models in combination with a lack of regulation (note: it has to be mentioned in this context though, that the 5. AMLD and Austria's corresponding implementation act stipulate regulatory requirements for select crypto-asset service provider). Continuous media reports and user-exchange in online-boards indicate that those risks have to be rated high.

Further concerns related to crypto-assets are

- upcoming new technologies (like quantum computing) or even existing technical possibilities, that could nullify existing cryptographic barriers used by DLT,
- compliance with the General Data Protection Regulation,
- problems when assigning technical and operational responsibility (or impose necessary technical measures) to an authorized entity caused by decentralized environment and
- various other aspects such as how to handle the loss of private keys and other currently hard to foresee issues which may materialise as the technology is adopted by a wider audience.

"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'*[25] 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).

12) **In our view, what are the benefits of "stablecoins" and "global stablecoins"? Please explain your reasoning (if needed).** [Insert text box]

Benefits and risks would depend on the specific business model. The risk profile of 'stablecoins' and conflicts with public interests are completely different if the issuer and manager of the ecosystem is a Central Bank compared to a private actor like the Libra Association. In this context an issue could derive from the issuance of (global) 'stablecoins' through BigTech providers with a large user base. This could bear potential for a certain amount of currency substitution as these companies already enjoy reliability. Consequently, emergence of parallel and private currencies on a global level issued by BigTechs could cause major risks and the overall monetary system could therefore be challenged. Furthermore, risks are generally linked to the basket of value acting as underlying for the stablecoin. In our point of view, it would be more beneficial to develop existing payment systems further with the aim to optimize financial inclusion, velocity, transparency and security of payments.

That being said and strictly hypothetically speaking, 'stablecoins', particularly global 'stablecoins', mostly promise to facilitate fast cross-border payments (without usual lags of settlement) and to increase financial inclusion, especially in emerging countries. These benefits are predicated on appropriate designs being capable of properly managing risks, fulfilment of oversight and other potentially relevant regulatory requirements. To our knowledge, though, there are as of yet still no global 'stablecoin' examples in circulation fulfilling these above mentioned "promises" sufficiently.

On another note, the term 'stablecoin' could be misleading as it implies that these coins are inherently more stable than others. It could suggest inherent stability mechanisms usually associated with official currencies. Furthermore, its use by regulators may give the false impression that the regulatory community endorses the credibility of this view. This could be problematic with regard to investor and consumer protection as much as for financial stability.

13) **In your opinion, what are the most important risks related to "stablecoins"? Please rate each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".**

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

	1	2	3	4	5	No opinion
Fraudulent activities					x	
Market integrity (e.g. price, volume manipulation.)					x	
Investor/consumer protection					x	
Anti-money laundering and CFT issues					x	
Data protection issues					x	
Competition issues					x	
Cyber security and operational risks					x	
Taxation issues					x	
Energy consumption	x					
Financial stability					x	
Monetary sovereignty/monetary policy transmission					x	
Other						x

Please explain in your answer potential differences in terms of risks between "stablecoins" and "global stablecoins" (if needed). [Insert text box]

'Stablecoins' still present themselves as a marginal phenomenon at the moment. Besides a historical peak of fascination and investment activity in July 2019 (presumed mostly due to the announcement of Facebook's Libra) there is virtually no relevant activity (transactions, trades, market volumes) to be observed with this form of crypto assets since. As mentioned in answer to question 11, Bigtech 'stablecoins' could potentially have an impact on global markets but this is also still an open debate without empirical or otherwise expedient experience.

Besides several open regulatory questions and from an institutional view, we see some important issues with stablecoins, especially when operating on global scale and outside of EU regulation. As such, major concerns revolve especially around the monetary sovereignty of nations, disadvantageous influence on currencies included in stable coin reserve baskets and unfavourable competition with established institutional payment systems.

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.

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**~~

Please explain your reasoning (if needed). [Insert text box]

The Ministry of Finance (MoF), the Austrian Financial Market Authority (FMA) and the OeNB are in discussions and information exchange with relevant stakeholders via the Austrian FinTech Advisory Board. The feedback we have received so far indicates that reputable companies would appreciate a framework to clearly set them apart from unprofessional and fraudulent ventures.

However, on a general note, the applicability and resilience of our current regulatory frameworks should be profoundly analysed in order to take the appropriate EU-level measures. If current legislation seems to be insufficient new tailored legislation could be considered. It should be further assessed if a code of conduct (e.g. including self-commitment rules respectively comply or explain) might have a positive effect.

Currently some crypto asset service provider struggle with uncertainties, which influences their ability to interact with traditional financial market participants. For instance the French ICO and digital asset service provider legislation ("PACTE" law) specifically includes the goal to offer objective, non-discretionary and proportionate rules for ICO issuers which have received the PACTE visa to open deposit and payment accounts (see: *Autorité des marchés financiers*, France's New Framework for ICOs and Tokens: Simple, attractive and protective https://www.economie.gouv.fr/files/files/2019/ParisEUROPLACE_FrancesNewFrameworkapril_2019.pdf).

A European framework might be best suited to create a level playing field across jurisdictions for crypto asset service provider and ensures a high level of consumer and investor protection. As crypto asset service providers are regularly conducting cross-border business, a passporting regime would be needed to facilitate a European Single Market.

The FMA endorses European legislation to harmonise the taxonomy of coins / token, to introduce a prospectus regime for ICOs / ITOs / IEOs and to create a European regulatory framework for digital asset service providers.

15) **What is your experience (if any) as regards national regimes on crypto-assets? Please indicate which measures in these national laws are, in your view, an effective approach to crypto-assets regulation, which ones rather not.** [Insert text box]

At this point in time there is no specific national legislation on crypto assets besides the transposition of European AML/CFT legislation into Austrian law. The Austrian Financial Market Authority (FMA) follows with interest the efforts of other Member States like the French PACTE legislation regarding ICOs and digital service asset provider or the Liechtensteinian TVTG Blockchain legislation. Although we share the opinion that crypto assets demand adaptions of existing financial market frameworks as well as specific new provisions to regulate crypto asset service provider, a European approach is needed.

Due to the digital nature of crypto assets, national regimes are not suitable to address the specific needs and risks linked to the crypto asset economy. A harmonised minimum standard for crypto asset service providers would facilitate cross border activity within the European Union, strengthen the European Single Market and create a level playing field in regards to consumer and investor protection. National regulation cannot offer passporting, leads to further fragmentation, undermines legal certainty of cross-border business and potentially causes a regulatory "race to the bottom" in an attempt to increase the attractiveness of national regimes for digital asset service provider.

The FMA endorses European legislation to harmonise the taxonomy of coins / token, to introduce a prospectus regime for ICOs / ITOs / IEOs and to create a European regulatory framework for digital asset service provider.

Furthermore, the legal assessment of tokens is regularly linked to legal terms stipulated by European law (e.g. "financial instrument" according to MiFID II or "electronic money" according to EMD 2). National regimes are unfit to provide legal certainty for issues which arise due to new technologies (like distributed ledger applications) being introduced into the scope of European financial services regulation. In order to enable innovative entrepreneurs to conduct their business on a sound legal basis in the European Single Market, a European approach is needed.

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,

The balance between facilitating market entry for innovative players and protecting customers and competitors is an issue not limited to crypto-assets but for all areas of innovation. Regulation shall definitely not be seen as obstacle for innovation. In our experience, regulation is facilitating innovation because regulation creates trust and lifts providers up to the level of well respected financial institutions. This generates advantages in funding, hiring the best experts and attracting customers. Furthermore, institutional investors may abstain from investing in unregulated businesses due to the potential compliance issue linked to the uncertain legal basis of the business model. However, the primary goals of financial market regulation are investor protection and financial stability. Regulators should therefore carefully take into account positive signalling effects of any new regulation and make sure that these effects do not jeopardize financial stability or investor protection.

The biggest burden is unclarity due to undefined legal status and legal fragmentation. The priority in regards to a new crypto asset law has to be harmonisation. A regulatory European crypto-asset framework needs to encompass existing European legislation (e.g. prospectus law regarding security token offerings, payment services regarding payment tokens that are already e-money, the new AML-regime for VASPs, the upcoming crowdfunding regulation, which will explicitly exclude ICOs without defining them).

If an evaluation of existing market regulation shows that the risks linked to crypto-assets are insufficiently covered by existing legislation, regulatory minimum requirements for crypto-asset services providers need to be introduced (see answer to question 7). The potential applicability and resilience of our current regulatory frameworks should be profoundly analysed in order to take the appropriate EU-level measures. If current legislation seems to be insufficient, new tailored legislation could be considered.

Crypto-assets should be addressed in existing financial market regimes (e.g. including Bitcoin et al into the e-money and payments regulation, naming crypto-assets as possible underlying for derivatives under the securities regulation etc) to address the issue of legal uncertainty. This would weave crypto assets smoothly into well established law that the markets already are familiar with and that already balance the interest of providers, competitors and customers.

The gatekeepers are the key players for a trustful environment and a sustainable development of crypto-markets. Exchanges, wallet-providers and trading-platforms should be the centre of the regulatory interest. If exchanges or wallet providers are regulated, then their regimes should follow comparable regimes (e.g. payment services providers or securities firms who are obliged to a sufficient funding, to transparency, to risk management, to AML-prevention, etc.). If a holistic crypto-asset service provider regime is deemed necessary, it needs to be coherent with existing rules for securities exchanges, commodity and currency exchanges, security depositors and other already regulated intermediaries (note: some crypto asset service provider are already subject to these regulations).

If a new regime is deemed necessary, the classification in payment, security, utility token could be upheld although it could also be considered to introduce a new cross-asset terminology into European legislation (see answer in question 7). Offers of crypto assets that only embody a right to access goods and services but no financial claims and no payment function, should not be included in a new regulation. However, any legal definition needs to be broad enough to include hybrid tokens, for instance utility token that change their functionality through their life cycle and gain investment and/or payment character.

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)
[Insert text box]

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[26]?**

- **Yes**
- ~~**No**~~
- ~~**Don't know/no opinion**~~

Please indicate how this clarity should be provided (guidance, EU legislation...).

At the moment there seems to be no observable investment appetite into crypto assets by credit institutes. As global findings of the Bank for International Settlements about banks' crypto asset exposures in December 2018 indicate, investment activities and exposures are immaterial to nearly non-existent (especially among EU banks). Latest internal Austrian banking surveys undertaken by OeNB (in December 2018) confirm that impression.

Nevertheless, we recommend that any initiatives for prudential treatment should integrate or link with already existing approaches and activities (eg: IFRS Committee on "holding of cryptocurrencies" and "meeting the definition of IAS 38 intangible assets" in June 2019, https://www.ifrs.org/projects/2019/holdings-of-cryptocurrencies/; or ESMA advice on initial coin offerings and crypto-assets from January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf). EBA (report and advice on crypto-assets 1/2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf) and ECB (occasional paper 223, 5/2019, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf?a31360223fb32f0e50a82ce649a8b7fc) already provided first statements on a conservative approach. The EBA still works on a guidance on the prudential treatment of institutions' holdings of/exposures to crypto-assets and the development of a common monitoring template (the delivery is delayed at the moment). Guidances of the other ESAs could follow if deemed necessary.

In our opinion clarity is very important. In order to achieve sufficient legal certainty and harmonization, EU-legislation seems to be needed. Complementary level 3 guidelines could be regarded as providing further clarification.

[26] See the discussion paper of the Basel Committee on Banking Supervision (BCBS) "Designing a prudential treatment for crypto-assets", dec 2019.

18) **Should harmonisation of national civil laws be considered to provide clarity on the legal validity of token transfers and the tokenization of tangible (material) assets?** [Insert text box]

Legislative initiatives to increase legal clarity concerning the legal effects of of innovative technologies in existing legislation may be supported. Considering the systematic differences in national civil codes, a European harmonisation seems very challenging. Nevertheless, Member States should clarify if transfer of ownership via blockchain and tokenization of tangible assets is possible in their respective jurisdictions.

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.

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?** [Insert text box]

Issuers (Initial Coin Offerings [ICO], Initial Exchange Offerings[IEO]), exchanges, ATM-providers, trading-platforms (primarily Contracts for Difference [CFD] on crypto-assets), telegram trading bots, payment services providers, providers of investment like service regarding crypto assets (investment advice or portfolio management, financial analysis on crypto assets) and Virtual Asset Service Providers (VASP).

In the absence of regulated entities and due to overlaps in business models, cross-border business from abroad and business models still in the planning stage, no specific numbers can be provided at this point in time.

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[27]. 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,

[27] Study from the European Parliament on "Cryptocurrencies and Blockchain", July 2018

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.

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**~~

Please explain your reasoning (if needed). [Insert text box]

Crypto assets issuers usually provide international services and regularly do not have a physical presence in the EU. Whitepapers are often intransparent and unclear. In many cases token are deliberately designed to not embody a legal claim or only embody a very limited legal claim against the issuer. For authorities it is difficult to pursue fraudulent activities and take necessary regulatory measures if natural persons behind these firms are unknown. From a purely prospectus law perspective, no physical presence in the EU is required for crypto-asset issuer.

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**~~

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 cryptoasset issuer, the project, the rights attached to the crypto-assets, on the secondary trading, the underlying technology, potential conflicts of interest.). [Insert text box]

On an introductory note, currently, one of the biggest challenges is the lack of adequate information of entities providing or planning crypto-asset initiatives, especially for security tokens. This makes it very difficult to reach definitive conclusions on whether and how the existing regulatory framework applies. Therefore involved players should be required to provide full and adequate information for investors and supervising authorities.

If a crypto asset constitutes a regulated instrument under the current or the future regulation the issuer of the crypto-asset should be obliged to provide clear information through an information document. Because terms and conditions of crypto assets are often unclear, rights and the risks are hidden through overlong provisions, minimum standards on coherence should be determined. Disclosure requirements for such assets should be standardized on EU level. The information should contain the following aspects (partially derived from the French PACTE law):

1. Name and address of the issuer in the EU
2. Contact information of the issuer in the EU
3. Description of the issuer
4. Project description
5. Characteristics of the issue
6. Rights attached to the crypto assets (e.g. fungibility, right of repayment)
7. Risk factors attached to the asset (e.g. no or limited right of repayment)
8. Discretion rights of the issuer
9. Functions of the Assets
10. Underlying instruments
11. Underlying technology/ Technical protocol procedures
12. Safeguarding of the assets
13. Number of Assets in total
14. Value of Assets at issuance
15. AML/CFT procedures
16. Applicable law

Issuers of crypto-assets could be subject to easements similar to the Prospectus Regulation (EU) 2017/1129 in terms of scope.

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 each proposal from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant". [insert text box]

	1	2	3	4	5	No opinion

The Consumer Rights Directive[28]					X	
The E-Commerce Directive[29]			X			
The EU Distance Marketing of Consumer Financial Services Directive[30]					X	
Other (please specify)						

Please explain your reasoning and indicate the type of clarification (legislative/non legislative) that would be required [insert text box]**.**

Consumer Rights Directive: applies to contracts between a trader and a consumer. According to Art 3 par (3) lit (d) it does not apply to financial services. Art 2 par (12) defines 'financial service' as "any service of a banking, credit, insurance, personal pension, investment or payment nature". This definition should be brought in line with the relevant definitions in financial markets law and examined with regard to the functionalities of utility tokens to increase legal certainty. Depending on how utility tokens / hybrid tokens are classified, the Directive would only apply to emissions of these types of tokens. Such offerings usually constitute a 'distance contract' according to Art 2 par (7). Hence, Articles 6 and 8 – 16 are applicable. Some of the information required in Art 6 cannot be provided by decentralized issuers. This should be addressed. Any information requirements imposed should take into account the right of withdrawal (Art 9). Some of the formal requirements for distance contracts (Art 8) could be adapted to create an information requirement regarding the payment/purchase process in the emission. As it stands, this process is generally handled automatically by a smart contract and is not transparent for technically inexperienced users. This is also relevant in regards to Art 10 par 1 lit (a) of the E-Commerce-Directive and the respective provisions in the EU Distance Marketing of Consumer Financial Services Directive.

The right of withdrawal poses a significant challenge. Any information requirement imposed should contain information on whether or not such a withdrawal right exists. Art 16 lit (b) exempts utility tokens that are tradeable on the secondary market within the withdrawal period from the right of withdrawal since their value can and will fluctuate on the secondary market, which the trader cannot control. Consumers should be informed about this fact and this information should be kept current in the case of ongoing emissions (tradeability may change over time).

E-Commerce Directive: applicable to provision of 'information society services': any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. According to Directive (EU) 2015/1535 Art 1 par (b) lit (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request. It should be clarified under which circumstances the transfer of a token-balance on a DLT system fulfils this definition (technically tokens are not "sent" to the users address).

Since the contract terms are often technically represented by smart contracts it should be clarified that access to the smart contract does not satisfy Art 10 par 3. This requirement should be satisfied by the whitepaper instead. Discrepancies between the whitepaper and smart contracts are not uncommon and should be addressed as well.

[28] [Missing in the CP PDF]
[29] [Missing in the CP PDF]
[30] [Missing in the CP PDF]

It should also be clarified how different types of token emissions regarding the mode of transfer of the tokens are handled with regard to Article 11 “Placing of the order”. There are emissions that use a smart contract which exchanges the emitted token without (or without much) delay for another crypto-asset. There are however also emissions that are closer to traditional online sales where e.g. a sum of money is transferred by the customer and subsequently tokens are transferred via manual DLT transaction. The mode of emission thus heavily impacts the practical implementation of Art 11.

Art 11 par 2. is problematic with regard to emissions using smart contracts. Commonly, the transaction is initiated by the customer through a manual DLT transaction to the smart contract address. It is a feature of many DLT systems that transaction cannot be corrected after being sent. They also cannot be reversed. It should therefore be clarified, that this mode of emission falls under the exemption of Art 11 par 3 – and that DLT-transactions are an “equivalent individual communication”. This may warrant a change to this legal definition since DLT-transactions are not bilateral. They are broadcast to the entire network and not necessarily directly to the recipient of the crypto-asset. It is therefore questionable whether they qualify as “individual” communication under the current definition.

The EU Distance Marketing of Consumer Financial Services Directive: For Art 2 par (b) see comment regarding the definition of “financial service” according to the Consumer Rights Directive. In case certain information requirements are implemented for whitepapers they should cover the information in Article 3 (especially par 2 lit (a)). It should also be considered to clarify whether or not the publication of a whitepaper on a website could satisfy Art 3 par 1 and Art 5 (especially Art 5 par 2). In practice transactions handled by smart contract often do not feature any interaction between issuer and buyer aside from the DLT transaction. It is also often technically not feasible to provide documents to consumers through this channel.

For Art 6 ‘right of withdrawal’ see the comments under Consumer Rights Directive. It should also be clarified how stablecoins, which may fall under the directive, are classified under Art 6 par 2 lit (a). Another question is whether or not a transaction through a smart contract emission may fall under Art 6 par 2 lit (c) as a contract whose performance has been fully completed by both parties at the consumer's express request before the consumer exercises his right of withdrawal, depending on the functionality of the token.

It should also be noted, that in many cases there is no bilateral communication between the issuer and consumers at all. Thus, the prerequisite of notification before exercising the right of withdrawal may have to be adapted for such transactions if they are deemed to fall under the Directive.

It stands to reason, that transaction costs for emissions (e.g. “Gas” used on the Ethereum Blockchain) are not to be refunded under Art 6f since the transaction is initiated by the consumer and the transaction costs are usually paid to the entire network. This makes a refund impractical and a significant burden on issuers.

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 each proposal from 1 to 5, 1 standing for “completely irrelevant” and 5 for "highly relevant ".

	1	2	3	4	5	No opinion

The managers of the issuer or sponsor should be subject to fitness and probity standards		x				
The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions		x				
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		x				
Other						

Please explain your reasoning (if needed). [Insert text box]

General remark
If crypto assets not covered under MiFID can be traded on public platforms, disclosure on an ongoing basis by the issuer will most likely be necessary similar to obligations of issuers on trading venues (regulated markets, MTFs, OTFs, see ongoing disclosure obligations in the Market Abuse Regulation and Transparency Directive – e.g. publication of inside information, managers' transactions, financial statements).

We understand that from an investors' perspective, buying and selling a crypto-asset on trading platforms works very similar to current financial markets. The price of a security token, which is not covered under MiFID, will likely depend on information, which can only be provided by the issuer (e.g. good earnings). This may apply also to other crypto-assets depending on its specific design. In order to make an informed decision on buying or selling a crypto-asset, the investor needs information.

We understand the intention to promote new technologies and leave freedom to the issuers. Currently the risks associated with crypto-asset issuers and sponsors are mitigated by the small volume of these markets compared to the financial markets. However, in the long run, if this industry becomes larger, it will be necessary to require ongoing disclosure at least for specific crypto-assets to protect investors.

Fitness and probity standards
In general, managers of issuers on the financial markets are not subject to fitness and probity standards. These rules currently only apply to specific entities (e.g. credit institutions, investment firms etc.) and should not be extended in scope to crypto-asset issuer unless similar risks are identified.

Misleading marketing
As long as misleading the public is prohibited we see no need for specific advertising rules.

Safeguard the funds
Again, we see no reason to make a difference between issuers on financial markets and crypto-asset issuers.

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).

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 (if needed). [Insert text box]

Criteria to differentiate between stablecoins and global stablecoins could be:

- Global distribution (stablecoins encompassing several jurisdictions)
- Business/reserve modell (size and risk of reserve, interconnectedness with the financial system)
- Potential large number of users
- BigTech involvement
- Perceived reliability as store of value
- Redemption value linked to multiple currencies
- Redemption value linked to foreign currency(s)
- Systemic relevance (potential to trigger or transmit systemic shocks)
- Potentially substantial cross border usage in payments and remittance

25) 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 <u>both “stablecoins” and “global stablecoins”</u> if each is proposal is relevant (leave it blank if you have no opinion).

	“Stablecoins”		**“Global stablecoins”**	
	Relevant	**Not relevant**	**Relevant**	**Not relevant**
The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short termgovernment bonds...)	X		X	
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	X		X	
The assets or funds of the reserve should be segregated from the issuer's balance sheet	X		X	

The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	X		X	
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	X		X	
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	X		X	
Obligation for the assets or funds to be held in custody with credit institutions in the EU	X		X	
Periodic independent auditing of the assets or funds held in the reserve	X		X	
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	X		X	
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	X		X	
Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer	X		X	
Other				

Please illustrate your response (if needed). [Insert text box]

In general, regulation should lean on the principles of technological neutrality and proportionality (same business, same risk, same rules). Business models should therefore be seen in relation to similar business models (similar in nature). Unspecified, maybe unclear and therefore probably disruptive new business models could otherwise be used to challenge and reevaluate existing regulation or legislation on case by case basis.

"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".*

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**~~

Please explain your reasoning (if needed). [Insert text box]

The purchase of stablecoins in large amounts (e.g. by crypto exchanges) and resale to retail investors is suitable for market manipulation. For this reason, an appropriate regulation preventing market manipulation should be created or the scope of the Market abuse Regulation (MAR) extended.

Keeping in mind the fact that all European capital market regulations (Prospectus Regulation, AIFMD, MiFID II, etc) meet different requirements with regard to sales to retail clients vs sales to professional clients/eligible counterparties/qualified investors etc, a corresponding approach seems appropriate within a potential legal framework for crypto assets and stable coins. It has to be mentioned in this context, that Austrian supervisory authorities are in favor of harmonizing the currently fragmented definitions and requirements in regards to professional clients in EU law.

However, this does not refer to the potential economic dangers of such types of stablecoins (see, for example, the intended design of "Libra") regarding money market policy, currency sovereignty or financial stability, which accordingly require an independent risk evaluation. These circumstances must be regulated autonomously and should not be mingled with other areas such as compliance with rules of conduct when distributing these assets.

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[31] while others use simple and inexpensive technology.

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 each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Absence of accountable entity in the EU					x	

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

Lack of adequate governance arrangements, including operational resilience and ICT security					x	
Absence or inadequate segregation of assets held on the behalf of clients (e.g. for 'centralised platforms')					x	
Conflicts of interest arising from other activities					x	
Absence/inadequate recordkeeping of transactions					x	
Absence/inadequate complaints or redress procedures are in place					x	
Bankruptcy of the trading platform					x	
Lacks of resources to effectively conduct its activities					x	
Losses of users' crypto-assets through theft or hacking (cyber risks)					x	
Lack of procedures to ensure fair and orderly trading					x	
Access to the trading platform is not provided in an undiscriminating way					x	
Delays in the processing of transactions					x	
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-a-vis the platform)					x	
Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse					x	
Other						

Please explain your reasoning (if needed). [Insert text box]

The typical risks of providers who administer OTC traffic of customer assets, which are not supervised, materialize.

The main risks correspond to the overall risks linked with DLT (number of unsolved issues linked to that technology – loss of keys; upcoming new technology that challenge cryptographic barriers, etc.). Apart from those basic risks linked with DLT, this technology seems to fit the role of a settlement system rather than a trading system. It seems unclear how the basic functions of a trading system (matching buyers and sellers) with its typical requirements of efficient and close to real-time trading can be performed "on chain" (particularly if the consensus protocol used is proof of work - based). As the term "ledger" suggests, the technology seems to be better equipped for transfer / custodian / safekeeping purposes.

From a regulatory perspective a separation between custodian / settlement services (via DLT) and the operation of a trading platform (via centralized systems "off chain") could possibly foster an orderly trading environment and therefore should be considered as part of regulation.

28) What are the requirements that could be imposed on trading platforms in order to mitigate those risks? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion

Trading platforms should have a physical presence in the EU					x	
Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					x	
Trading platforms should segregate the assets of users from those held on own account					x	
Trading platforms should be subject to rules on conflicts of interest					x	
Trading platforms should be required to keep appropriate records of users' transactions					x	
Trading platforms should have an adequate complaints handling and redress procedures					x	
Trading platforms should be subject to prudential requirements (including capital requirements)					x	
Trading platforms should have adequate rules to ensure fair and orderly trading					x	
Trading platforms should provide access to its services in an undiscriminating way					x	
Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse					x	
Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)					x	
Trading platforms should be responsible for screening crypto-assets against the risk of fraud					x	
Other						

Please indicate if those requirements should be different depending on the type of crypto-assets traded on the platform and explain your reasoning (if needed). [Insert text box]

Trading platforms that trade security tokens would already be subject to all those obligations under existing law because they would trade financial instruments according to MiFID II. But also all other crypto-assets that are tradable and therefore have a market value are prone to risk. If someone's main business is trading and transaction administration (by forwarding the order to an exchange, to take it on the own book, by matching, by any other way of executing orders) this should be subject to regulation because it can affect a broader range of customers.

To avoid an unlevel playing field with typical online-merchants, platforms that trade plain utility token should not be subject to the same regulation - these should be subject to the rules for the trading of goods and services. If a crypto-asset has hybrid functions, i.e. an investment or payment component is an equivalent (main) feature, then it should be included in the existing regulatory framework.

As suggested in question 7 a horizontal regulation which includes a broad definition for crypto-assets and regulatory requirements for specific activities and services linked to this definition seems like the most efficient legislative approach. Any platform trading a crypto-asset which embodies a financial claim and/or is used for payments at third parties would fall under the regulatory scope. Trading platforms trading security tokens which are financial instruments have to comply with the provision laid down in the MiFID II-regulation (lex specialis). Trading platforms which are trading other kinds of tokens (e.g. plain utility tokens) would fall outside and constitute e.g. a commodity exchange.

It should be kept in mind that the whole concept of regulation has been based upon authorization and supervision – both of which require the applicant or supervised entity to be capable of operating, adjusting and governing the arrangements and systems used when providing their services. It seems unclear how regulatory concerns might be addressed with that regard in cases of decentralized systems. One of the key requirements therefore should deal with the providers capability of performing (when needed also substantial) adaptations to the systems used when necessary – for instance when new technologies arise that make the present technical systems unsafe. It is important that regulatory requirements are detailed and precise in addressing regulatory issues of the DLT (for instance taking into account the different consensus protocols, e.g.proof-of-work and proof-of-stake). Unspecific "high level" provisions are insufficient to address the problem of legal uncertainty and are not able to guarantee a level playing field among service providers.

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[32].

29) In your opinion, what are the main risks in relation to crypto-to-crypto and fiat-to-crypto exchanges? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

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

Please explain your reasoning (if needed). [Insert text box]

The listed risks are typical risks of unsupervised entities that handle money and assets on a larger scale. Some of the risks mentioned above (e.g. recordkeeping of transactions, information about crypto assets) are already covered – to some extent – by AML/CFT regulation for Virtual Asset Service providers (including exchanges), both on an EU level (5. AMLD) and on an international level (revised FATF Standards).

The main risks associated with exchanges differ and depend on the exact kind of offered services (e.g. broker/dealer services also providing custodial wallet providers).

30) What are the requirements that could be imposed on exchanges in order to mitigate those risks? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Absence of accountable entity in the EU					x	
Exchanges should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					x	
Exchanges should segregate the assets of users from those held on own account					x	

[32] Study from the European Parliament on "Cryptocurrencies and Blockchain", July 2018

Exchanges should be subject to rules on conflicts of interest					x	
Exchanges should be required to keep appropriate records of users' transactions					x	
Exchanges should have an adequate complaints handling and redress procedures					x	
Exchanges should be subject to prudential requirements (including capital requirements)					x	
Exchanges should be subject to advertising rules to avoid misleading marketing/promotions					x	
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)					x	
Exchanges should be responsible for screening crypto-assets against the risk of fraud					x	
Other						

Please indicate if those requirements should be different depending on the type of crypto-assets available on the exchange and explain your reasoning (if needed). [Insert text box]

Crypto-Exchanges are one of the most important „gate keepers“, so they should be subject to regulation (which is already achieved in regards to AML/CFT obligations). Crypto-Exchanges are the place where market integrity risks grow; malversations and insolvencies have potentially great impact.

A differentiation by nature of the crypto-assets in this regard seems hard to administer. Furthermore, the trading of payment, hybrid and no-business-token can result in similar financial risks for customers like the trading of security tokens. However, from a proportionality standpoint a differentiation in the regulatory approach in regards to plain utility token seems reasonable. A legal framework for commodity exchanges already exists; a future regime for plain utility tokens should be similar constructed from a supervisory standpoint. Otherwise, there would be the risk to create an unlevel playing field compared to other forms of digitalized assets (e.g. purchasing concert tickets via an online-platform – the tickets embodies the financial value of a utility and are tradable assets. The only difference to a “Ticket-Token” traded on a crypto-exchange would be the usage of DLT). Keeping the desire to establish Europe as innovative-friendly market in mind, a regulatory approach which burdens business transactions with regulatory requirements solely because a specific technology is used, seems undesirable.

Generally it seems favourable to define a single crypto-asset-class (instead of the commonly trisection of payment / investment / utility token) as described in question 7 and 28. In this context it is important to note, that the same regulated activities need to follow the same regulatory requirements regardless of the specific technology used.

4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys[33] 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[34]. 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.

31) In your opinion, what are the main risks in relation to the custodial wallet service provision? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
No physical presence in the EU					x	
Lack of adequate governance arrangements, including operational resilience and ICT security					x	
Absence or inadequate segregation of assets held on the behalf of clients					x	
Conflicts of interest arising from other activities (trading, exchange)					x	
Absence/inadequate recordkeeping of holdings and transactions made on behalf of users					x	
Absence/inadequate complaints or redress procedures are in place					x	
Bankruptcy of the custodial wallet provider					x	
Inadequate own funds to repay the consumers					x	
Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)					x	
The custodial wallet is compromised or fails to provide expected functionality					x	
The custodial wallet provider behaves negligently or fraudulently					x	
No contractual binding terms and provisions with the user who holds the wallet					x	
Other						

[33] 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.

[34] 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.

Please explain your reasoning (if needed). [Insert text box]

Like crypto-exchanges, wallet-provider are key gatekeepers for crypto-markets. In economic environments based on asymmetric cryptography the access to private keys determines the access to customer's assets. Customers regularly depend completely on their wallet-provider. Therefore malversations and a lack of diligence have the potential to impact markets in a major way. The increasing relevance off-wallet-providers for the crypto-ecosytems causes an increasing demand for customer and market protection through regulation. As mentioned above in the context of exchanges (see question 29), some of the quoted risks (e.g. recordkeeping of transactions, information about crypto assets) are already covered – to some extent – by AML/CFT regulation for Virtual Asset Service providers (including wallet providers), both on an EU level (5. AMLD) and on an international level (revised FATF Standards).

32) What are the requirements that could be imposed on custodial wallet providers in order to mitigate those risks? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Custodial wallet providers should have a physical presence in the EU					x	
Custodial wallet providers should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					x	
Custodial wallet providers should segregate the asset of users from those held on own account					x	
Custodial wallet providers should be subject to rules on conflicts of interest					x	
Custodial wallet providers should be required to keep appropriate records of users' holdings and transactions					x	
Custodial wallet providers should have an adequate complaints handling and redress procedures					x	
Custodial wallet providers should be subject to capital requirements					x	
Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions					x	
Custodial wallet providers should be subject to certain minimum conditions for their contractual relationship with the consumers/investors					x	
Other						

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 (if needed). [Insert text box]

The safekeeping of securities is already regulated, as well as the custody of e-money (this would constitute a deposit business). If a new regime for custody of crypto-assets is created, than it has to harmonize with those regimes. On the other hand, there is the wide area of storage/custody of digitalized assets (software, pictures, music, identity) that is currently outside any regulation (besides of mere trade licenses) and should not be included in the future. The usage of DLT alone should not trigger additional regulatory requirements, there needs to be a level playing field between service provider offering similar services (e.g. the applicable law for keeping custody of an artwork should be the same – it should not matter if the service is performed by a regulated wallet-provider or an unregulated online-store).

If the trisection of crypto-assets is upheld, than custody services for payment, hybrid and no-use-tokens could become regulated activities. On the other hand the custody of plain utility token should not become a regulated activity.

A likely more efficient way from a regulatory perspective would be the introduction of a single crypto-asset-class (instead of the commonly used trisection) as elaborated in question 7 and 28.

With regard to AML/CFT obligations, the provisions of the 5. AMLD and the FATF standards already cover wallet providers.

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**~~

Please explain your reasoning (if needed). [Insert text box]

Custodial wallet providers should be authorised to offer custodial services for financial instruments if the same regulatory standards are applicable that non-crypto-asset businesses need to adhere to perform custodial services (e.g. safekeeping and administration of securities for other parties according to CRD IV). If the same regulatory standard is upheld, than there is no reason to prohibit custodial service providers from offering these services.

With regard to AML/CFT obligations, the provisions of the 5. AMLD and the FATF standards already cover wallet providers.

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? [Insert text box]

Transfer services from one wallet to another.

5. Other service 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.

35) In your view, what are the services related to crypto-assets that should be subject to requirements? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant"[35].

	1	2	3	4	5	No opinion
Reception and transmission of orders in relation to crypto-assets			x			
Execution of orders on crypto-assets on behalf of clients			x			
Crypto-assets portfolio management				x		
Advice on the acquisition of crypto-assets		x				
Underwriting of crypto-assets on a firm commitment basis			x			
Placing crypto-assets on a firm commitment basis			x			
Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)	x					
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)	x					
Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)			x			
Services provided by developers that are responsible for maintaining/updating the underlying protocol	x					
Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)	x					
Other services						x

[35] 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 illustrate your response, by underlining the potential risks raised by these services if they were left unregulated and by identifying potential requirements for those service providers. [Insert text box]

Technical activities alone should not be regulated (e.g. mining, validating, wire-transferring them). Regarding non-technical activities a differentiation according to the crypto-asset-class seems adequate. Note: security tokens that qualify as transferable security have to fulfill all of the proposed requirements already, due to the fact that they are subject to MiFID II. The mentioned requirements are inspired by MiFID II, nevertheless they may not be adequate for payment or hybrid tokens. A reception and transmission of orders in relation to payment and utility tokens would create unreasonable differences to businesses related to payment instruments / means of payment and utilities that are not tokenized.

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)[36], 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.

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**~~
- **Partially**
- ~~**Don't know/no opinion**~~

Please explain your reasoning (if needed). [Insert text box]

This would require a case-by-case analysis. A crypto asset, which can only be redeemed against the issuing company and thus is similar to a voucher for services or goods, has to be treated differently, than crypto-assets with payment and/or investment function.

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

[36] Payment Services Directive 2 (2015/2366/EU)

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.

37) In your opinion, what are the biggest market integrity risks related to the trading of crypto-assets? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Price manipulation					x	
Volume manipulation (wash trades...)					x	
Pump and dump schemes					x	
Manipulation on basis of quoting and cancellations					x	
Dissemination of misleading information by the cryptoasset issuer or any other market participants					x	
Insider dealings					x	
Other						

Please explain your reasoning (if needed). [Insert text box]

All of the above mentioned risks have to be rated as “highly relevant”.
The whole concept of the MiFID II/MiFIR and CSMAD/MAR package was to increase transparency of financial markets, to smooth functioning of securities markets and public confidence in the markets. Investor protection is another important issue. FMA is of the opinion that these fundamental concepts hold true for each and every market related to behaviors/transactions/orders etc. similar to those possible with regards to financial instruments. Having said that the named risks qualify as risks undermining the mentioned fundamental concept.

It should be noted that processes are currently taking place in the crypto assets space that conflict with the relevant legal provisions in the context of European capital market law. Examples include processes related to the artificial shortage of (emitted) crypto assets (for example token “burn” events) in order to initiate an increase in the value of the asset. In the context of a potential bespoke regime for crypto assets, which cannot be classified as financial instruments under MiFID II, such practices would have to be captured in a regulatory manner similar to the existing market integrity regime.

While market integrity is the key foundation to create consumers’ confidence in the cryptoassets market, the extension of the Market Abuse Regulation (MAR) requirements to the crypto-asset ecosystem could unduly restrict the development of this sector.

38) **In your view, how should market integrity on crypto-asset markets be ensured?** [Insert text box]

Depending on the decision whether crypto-assets are qualified as financial instruments or not, a different amount of new legislation is needed to ensure market integrity. If they are explicitly qualified as financial instruments under MiFID II all provisions ensuring market integrity coming out of several European Acts (such as MiFID II/MiFIR, CSMAD/MAR, as well as all linked Level I – III Acts, etc.) will be applicable. If they are not qualified as financial instruments, it will need greater effort to build up a similar system ensuring market integrity, the functioning of the market, confidence of the investors and investor protection as it is now stipulated for the financial markets.

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).

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**~~

Please explain your reasoning (if needed). **If yes, please explain how you would see this best achieved in practice.** [Insert text box]

Assuming that similar provisions with regards to misconduct are introduced, it is essential for investigators to know who exactly is responsible for the breach of the rules. In order to ensure enforcement and sanctioning, it is important to formally identify the parties involved in the entire crypto-asset transaction process. On top of that each and every jurisdiction in the EU has the power to freeze or sequestrate assets. This can – at least according to our understanding – only be achieved through far reaching rules regarding identification of the participants, as well as reporting mechanisms throughout the whole transaction process.

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?** [Insert text box]

FMA is of the opinion that legislative requirements to ensure the proper identification of transactions are a global issue. Without similar provisions on a global basis it will be nearly impossible to effectively ban the circumvention of identification provisions due to the possibility to trade on platforms / exchanges in third countries. Especially without having global harmonization according to the above mentioned provisions close cooperation of the responsible authorities is needed. Last but not least it is important to keep in mind that even with identification provisions in place, there will be market participants willing to break the law. In this case authorities only have the possibility to issue acts of general prevention / for specific deterrence by sanctioning on a case by case basis.

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[37], 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'*[38]*.* 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.

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 'cryptoassets' that could be used in a potential bespoke regulation on cryptoassets)?

- ~~**Yes**~~
- **No**
- ~~**Don't know/no opinion**~~

[37] Anti-Money Laundering Directive (Directive 2015/849/EU) as amended by AMLD5 (Directive 2018/843/EU)
[38] FATF Recommendations

Please explain your reasoning (if needed). [Insert text box]

The above quoted definition of a virtual currency is from an old draft version of the 5. AMLD. The agreed upon definition of the 5. AMLD (Art. 3 no. 18) refers to a virtual currency as *"[…] accepted by natural or legal persons as a **means of exchange** and which can be transferred, stored and traded electronically"*. Therefore, the final version of the 5. AMLD does not use the narrower term of *"as a means of payment"* but uses a broad term *"to cover all the potential uses of virtual currencies"* (recital 10 5. AMLD). In our view, the EU legal framework uses the same broad definition for virtual currencies as the FATF. There is no necessity for an alignment with regard to the definition of virtual currencies.

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.

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? If any, please describe the possible risks to tackle. [Insert text box]

The EU AML/CFT legal framework should be extended to include all Virtual Asset Service Providers as defined by the FATF. First of all, this is necessary to ensure a level playing field on an European as well as on an international level.

Secondly, it is essential to make sure that all jurisdictions transpose the relevant FATF standards and develop regulatory/supervisory responses for all Virtual Asset Service Providers as defined by the FATF. All of these Virtual Asset Service Providers can be used for ML/TF purposes and therefore constitute a risk.

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**

Please explain your reasoning (if needed). [Insert text box]

In our view, this depends on what other crypto-asset service providers than those covered by the FATF-Standards are meant. As mentioned under question 42 we support an extension of the current EU AML/CFT legal framework to include all crypto-asset service providers as defined by the FATF. However, not every single person/entity with some form of connection to crypto assets should be an obliged entity under the EU AML/CFT legal framework. FATF put a lot of effort in its definition of Virtual Asset Service Providers and who should be covered by the FATF-Standards. The goal was to establish a comprehensive framework for the prevention of ML/TF with regard to crypto-assets and cover all relevant players without extending the AML/CFT-obligation too broadly.

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? [Insert text box]

One possible mitigation measure may be to compel parties in peer-to-peer transactions to include originator and beneficiary information in the transaction (i.e. to extend the so called "travel rule" from Rec. 16 of the FATF-Recommendations to peer-to-peer transactions). This wouldn´t be too much of a burden for "non-service providers" but would abolish anonymous transaction on a peer-to-peer level.

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."*[39]

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**~~

Please explain your reasoning (if needed). [Insert text box]

[39] FATF Recommendations

In our view, it is of utmost importance to include this obligation in the EU AML/CFT legal framework for crypto-assets. This is one of the major obligations to tackle anonymity of transactions and create some form of “paper-trail” for necessary investigations.

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 each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
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					x	
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					x	

Please explain your reasoning (if needed). [Insert text box]

The above-mentioned requirements are important obligations in every comprehensive AML/CFT framework. Therefore, these requirements should also be a condition for the registration of crypto-asset service providers.

3. Consumer/investor protection[40]

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[41]. 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

[40] 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.
[41] ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019

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.

47) What type of consumer protection measures could be taken as regards crypto-assets? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Information provided by the issuer of crypto-assets (the so-called 'white papers')					x	
Limits on the investable amounts in crypto-assets by EU consumers	x					
Suitability checks by the crypto-asset service providers (including exchanges, wallet providers.)	x					
Warnings on the risks by the crypto-asset service providers (including exchanges, platforms, custodial wallet providers.)				x		
Other						

Please explain your reasoning and indicate if those requirements should apply to all types of crypto assets or only to some of them. [Insert text box]

On a general note, the applicability and resilience of our current regulatory frameworks should be profoundly analysed in order to take the appropriate EU-level measures. If current legislation seems to be insufficient new tailored legislation could be considered.

Regulatory requirements regarding whitepapers: Currently, whitepapers are the most important source of information in the market. Minimum requirements regarding content and form could be imposed to improve information in the market. The requirements should be tailored to the type of crypto-asset. However, as pointed out before, priority should be given to clarity regarding whether crypto-assets are covered by existing financial market regulation and therefore whether existing information obligations apply.

Limits on investable amounts: The crypto-economy is an international phenomenon. It is very simple to use crypto-exchanges outside EU-jurisdiction. Due to pseudonymity such limits would also be very hard to enforce. Limits may work in the traditional financial sector but they do not seem suited to the crypto-economy.

Suitability checks by the crypto-asset service providers: This proposal seems problematic and does not differentiate between types of crypto-assets or the type of service provided. Suitability checks are required by MiFID II only for investment advice and portfolio management regarding financial instruments. It would go against the principle of technology neutrality to impose this regulatory burden on all types of activities and crypto-assets only because of the technical implementation of the asset. Especially real utility assets without an investment function should not be treated like financial instruments. Such checks would also require a lot of information about the customer. It should also be noted that even under MiFID II the emission of securities does not fall into the scope of the regulation. Imposing such rules on crypto-issuers would create an unlevel playing field based solely on the technical implementation of a financial instrument.

Warnings: It makes sense to address (in case of payment services / financial instruments) those service providers who are already under supervision. It is however, again, questionable how to apply such rules to real utility tokens without an investment function. This type of crypto-assets comes in a myriad of forms – many of which do not in any way resemble products of financial markets (many of them are not even tradeable). We therefore strongly urge the Commission to carefully differentiate between types of crypto-assets in any and all considerations regarding regulation of the crypto-economy. A material issue with such warnings is also that one of the main risks associated with crypto-assets is the issuer risk / credit risk. Due to how fragmented and decentralized the market is, it seems problematic to require service providers such as wallet-providers to assess such risks. This type of information is usually not readily available for crypto-asset service providers, as it is not needed for their core business. Without this information however, warnings could only be very generic.

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**~~

Please explain your reasoning (if needed). [Insert text box]

Security tokens should, in principle, carry the same regulatory burden as any other traditional financial instrument. The same goes for payment tokens that fall under the EMD 2, PSD 2 or the CRR / CRD IV.

Payment tokens (e.g. Bitcoin) that are not regulated at the moment should be considered carefully. The goal should be to achieve a similar level of consumer protection while respecting the differences to regulated payment tokens (e.g. no central issuer, thus requirements for issuers make little sense).

Stablecoins should be treated like the type of instrument they are classified as (possibly a UCITS / AIF, security / financial instrument, regulated payment service).

Utility token are an extremely diverse type of token. The most important differentiation is between such utility token that have an investment purpose (e.g. early stage investment into pre-functional networks for speculation on secondary markets without a present use case for the token) and other utility tokens that do not have an investment purpose (e.g. vouchers for services / goods that are not tradeable or are tradeable but can already be used in the ecosystem thus limiting speculation due to a link to an actual good / service). The former should be treated similarly as security tokens while the latter should not be regulated at all (EU consumer protection law is applicable anyways) if there are no similarities to 'traditional' financial products.

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 *'airdrop')*[42].

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**~~

Please explain your reasoning (if needed). [Insert text box]

[42] See Autorite des Marches Financiers, French ICOs - A New Method of financing, November 2018

In principle, yes. The types of customers targeted and the relationship between issuer and customer differ greatly between private and public sales (see e.g. treatment in the prospectus directive). However, prevention of possible circumvention of the Prospectus Regulation through, e.g. questionable use of exemptions regarding the distribution to retail clients in private offerings has to be ensured.

As a side note, we also encourage the Commission to analyse the impact of the (technical) process of the emission on potential regulation. There are two main ways a crypto-emission may be conducted: (1) through a smart contract – basically an automated exchange crypto-asset for crypto-asset (2) through a manual DLT transaction – the customer transfers either FIAT-currency or Crypto-Assets to an account and the issuer manually transfers the crypto-assets to the customer.

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**~~

Please explain your reasoning (if needed). [Insert text box]

Yes, as long as no liabilities/obligations come with the crypto-assets. Gifts and donation do not constitute regulated services in capital markets law, e.g. under MiFID a gift does not count as a sale. This is logical since a true gift does not entail any risk of loss for the recipient. Additionally, we are of the opinion that regulating Air Drops (a market practice to send free crypto-assets to network users as marketing tool), as long as they are not used to circumvent supervision, would potentially end this practice since at the moment Air Drops are essentially a free marketing tool for DLT-based business models. Administrative effort and regulatory costs would make this model unfeasible. It should also be noted, that Air Drops may technically be directed at addresses that did not participate in the primary market transaction (i.e. token sale) – smart contracts used for Air Drops often drop to all addresses holding a balance in a specific token or based on mail-lists. This means that addresses could receive such tokens from secondary market transactions outside of the control of the issuer. That being said, issuers neither have the necessary information about the owners of such addresses nor do they have a means of communicating with them to provide them with information or comply with many other consumer protection laws.

One relevant exception from this are cases where Air Drops are used to fulfil financial market-related duties and obligations. Air Drops could e.g. be used to pay out dividends to shareholders.

It should also be noted that if a crypto-asset is traded speculatively, this practice could be considered an aggressive marketing technique and inappropriate practice, i.e., offering of payments, monetary or non-monetary benefits, as was the case with CFDs.

The vast majority of crypto-assets that are accessible to EU consumers and investors are

currently issued outside the EU[43]. 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.

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 each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".

	1	2	3	4	5	No opinion
Those crypto-assets should be banned					X	
Those crypto-assets should be still accessible to EU consumers/investors						X
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						X
Other						

Please explain your reasoning (if needed). [Insert text box]

Crypto-assets, that fall under existing EU Regulation but do not comply with it, should be banned in order to avoid a discrimination of EU companies issuing crypto-assets. Moreover, a regime that would only capture a minority of crypto assets might be ineffective. However, a ban must be legally enforceable.

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[44]. 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 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

[43] In 2018, for instance, only 10% of the crypto-assets were issued in the EU (mainly, UK, Estonia and Lithuania) - Source: Satis Research.
[44] https://www.ecb.europa.eu/pavm/pol/html/index.en.html

empowering the European Authorities (e.g. in cooperation with the European System of Central Banks) to supervise and oversee cryptoasset 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.

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 (if needed).** [Insert text box]

53) **Which are the tools that EU regulators would need to adequately supervise the crypto-asset service providers and their underlying technologies?** [Insert text box]

ESAs and NCAs need adequate resources (e.g. experts in the field of DLT and smart contract - analysis).

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[45] 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[46], 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[47] and on a preliminary legal assessment carried out by Commission services on the applicability and

[45] Trading venues are a regulated market, a multilateral trading facility or an organised trading facility
[46] European Markets Infrastructure Regulation (648/2012/EU)
[47] ESMA, 'Advice on Initial Coin Offerings and Crypto-Assets', January 2019

suitability of the existing EU legislation (mainly at level 1)[48] on trading, post-trading and other financial services concerning security tokens, such as asset management, the purpose of this part of the consultation is to seek stakeholders' views on the issues identified below that are relevant for the application of the existing regulatory framework to security tokens.

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

Current trends concerning security tokens

For the purpose of the consultation, we consider the instances where security tokens would be admitted to trading or traded on a trading venue within the meaning of MiFID. So far, however, there is evidence of only a few instances of security tokens issuance[49], with none of them having been admitted to trading or traded on a trading venue nor admitted in a CSD book-entry system[50].

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[51]. 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[52] 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[53] 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

[48] 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.

[49] For example the German Fundament STO which received the authorisation from Bafin in July 2019

[50] See section IV.2.5 for further information

[51] 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.

[52] 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.

[53] 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.

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.

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)?** [Insert text box]

Gold Coin: The subject crypto-asset was designed in such a way that its (basic) value would have been tied to the market price of gold. An issued token (ERC20) was equivalent to one gram of fine gold. The token holders would have had a debt redemption right to the issuer so that they would have been reimbursed the current gold price or physical gold (if a certain amount would have been exceeded). Due to the security-like design and functions, the FMA qualified this stablecoin as a transferable security as defined in Article 4(1)(44) of MiFID II and therefore as a financial instrument pursuant to Article 4(1)(15) of MiFID II.

As a result, the company decided not to implement the project in this way, but to offer customers a modified product. This was a non-transferable and non-tradable database entry in the corporate local network that only reflected ownership of the physical gold. On the basis of this adaptation, the product ceased to be classified as a financial instrument within the meaning of Article 4(1)(15) of MiFID II.

Crowd Funding Token: An entity planned to extend its crowdfunding infrastructure by issuing various tokens using blockchain technology and to make it accessible to others. Tokens were planned for payment on the platform (ICO), company tokens as issuances for the crowd funding projects designed in the form of subordinated loans, and an investor token for customer identification purposes. In particular the company tokens that were planned, embodying the subordinated loans are securities as defined in Article 4(1)(44) of MiFID II and therefore as a financial instrument pursuant to Article 4(1)(15) of MiFID II.

Digital Stocks: A company plans to buy stocks on its own account and issue token to customers. The price for the sale and the purchase of the tokens would be the price of the stock linked to the token. The token would not be transferable among the customers, but resellable to the company: The FMA classified these token as financial derivatives under MiFID II (Annex I Section C (4)). The company intended to offer this product through a 100% subsidiary company. According to our legal qualification the subsidiary company needs a license for reception and transmission of orders in relation to one or more financial instruments (MiFID II (Annex I Section A (1))

Crypto Index: A crypto exchange plans to offer an index product, which customers can use to buy crypto assets according to the allocation key of the index. For example, a customer may buy the product for EUR 100, which consists out of two values, Bitcoin (60%) and Ethereum (40%). The customer would therefore purchase Bitcoin for EUR 60 and Ethereum for EUR 40. The customer gains ownership over the crypto assets, which are stored in an "index wallet". The index wallet can be sold as a whole or pro rata. The company plans to start with three indices, which represent the Top 5, Top 10 and Top 25 crypto assets. The indices will be bought from a third party and should be periodically adjusted to market capitalization. The rebalancing takes place according to the weighting of the index provider.

According to our legal qualification, this business model does not constitute any already at EU-level regulated instrument, but an investment according to the Austrian Capital Market Act 2019 (national regulation); if no exception provisions are applicable.

Stablecoins & Smart Contracts: One company presented the following business model: The system connects the banking network (SEPA) with the ethereum blockchain. The company's customers are companies, i.e. real estate firms or FinTechs, which use Smart Contracts in their own client relationship. The company acts like a financial intermediary - it "moves" funds without using existing payment networks, purely on the blockchain, using their own stablecoin. The customers' client transfers Fiat-currency to the company's transaction account. The Fiat-currency will be converted immediately into the company's own stablecoin, which can be used in Smart Contracts. The stablecoin can be changed back to Fiat anytime by customers manually or by Smart Contracts. This enables a real estate firm to use smart contracts for real estate transactions. Neither the company's customers nor the customer's client need their own wallets or need to hold cryptocurrencies on their own in order to be able to interact with the blockchain application.

The company was not clear about the possibility to trade the stablecoin. There is no trading on third-party exchanges but the company provides its own „exchange platform", therefor it should be possible to transfer the stablecoin between existing clients.

There is no final assessment, but the FMA considered it possible that (i) holding the Fiat-money on the transaction account is a deposit business, (ii) the stablecoin is within the scope of the Payment Services Act 2018 and / or E-Money Act 2010 and (iii) the stablecoin might be a financial instrument pursuant to the MiFID II Directive.

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	X
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed). If you agree, please indicate the specific areas where, in your opinion, the technology could afford most efficiencies when compared to the legacy system. [Insert text box]

Several financial service providers, especially in the area of crowdfunding, are perceived as actively working towards digital issuance and settlement of tokens. There are already prototypes which show benefits and efficiencies in post-trading.
Main gains in efficiencies are expected in regards to the factors cost and time. Nevertheless disadvantages arising from the useage of DLT need to be considered in this context as well.

DLT systems in the form of (public-permissonless) blockchain systems primarily represent advantages in the post-trade area with regard to the speed of settlement of on-chain transactions as well as in terms of publicity and transaction traceability ("pseudo-anonymity").

Naturally with new technologies compared to settled legacy solutions, there are risks involved. But generally, complex reconciliation processes, counterparty and settlement risk as well as systemic risks (eg: bank runs) could be substantially improved (cost cutting, realtime-DVP, etc.) by well-designed DLT (Bindseil elaborates a very good example for a well-designed CBDC idea in ECB Paper Series No 2351/ Jan 2020).

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	X
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

The risk that needs to be addressed in the first place in the area of post-trade settlement is that - due to the architecture of DLT systems - there is no tangible entity that would be liable in the event of a dysfunction. It should also be borne in mind that in current DLT systems the unchangeability of transactions confirmed in the decentralized consensus is a reality. The reversal of potentially incorrect transactions would therefore be difficult or rather impossible. In addition, most DLT systems are based on the proof-of-work (PoW) consensus mechanism. The continuous security of PoW is difficult to assess on the basis of current information (for example with regard to developments in the field of quantum processors). These developments would potentially also question the security of computer systems that are not based on cryptographic encryption and would therefore pose a general security risk.

Regarding mass transactions, problems and challenges occurring with DLT (mostly performance and energy cost issues) are still not completely researched.

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. [Insert text box]

Based on available information, it is still too early for any judgements about this kind of technology (still mostly in research phase, no wide-spread adoption yet).

Also see answers to questions 55 and 56.

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	X
Rather agree	
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

Appropriate regulatory guidance at the European level would be of the utmost importance for both market participants and supervisory authorities, in order to ensure a harmonized approach in this area and to prevent further fragmentation through national solo efforts as well as to address potential risk areas and to contain them.

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)[54] and a regulation (MiFIR)[55] and their delegated and implementing 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[56] 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

[54] Market in Financial Instruments Directive (2014/65/EU)
[55] Markets in Financial Instruments Regulation (600/2014/EU)
[56] ESMA, 'Advice on Initial Coin Offerings and Crypto-Assets', January 2019

‘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.

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	X
Rather agree	
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

Legal uncertainty is always an impediment but much has been done lately to clarify the qualification of security tokens as financial instruments according to MiFID II. Due to common terms under MiFID II the qualification among the European authorities should not vary. Many authorities also established query systems within their innovation hubs to improve legal clarity.

Nevertheless, the regulations, for example with regard to transferable securities (and thus also indirectly with regard to security tokens) are largely shaped by national provisions (for example in the area of civil law), some of which differ widely. Appropriate measures at European level could create clarity and consistency in this area.

60) If you consider that this is an impediment, what would be the best remedies according to you? Please rate each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".

	1	2	3	4	5	No opinion
Harmonise the definition of certain types of financial instruments in the EU					x	
Provide a definition of a security token at EU level					x	
Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token					x	
Other						

Please explain your reasoning (if needed). [Insert text box]

A legally binding definition of a security token is important if the term itself has legal consequences. If the crucial term is financial instrument and thus the question is, under what conditions a security token is one, then the focus should be on guidance regarding the legal qualification.

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 each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".

	1	2	3	4	5	No opinion
Hybrid tokens should qualify as financial instruments/security tokens				x		
Hybrid tokens should qualify as unregulated cryptoassets (i.e. like those considered in section III. of the public consultation document)	X	-				
The assessment should be done on a case-by-case basis (with guidance at EU level)					x	
Other						

Please explain your reasoning (if needed). [Insert text box]

It has to be decided on a case-by-case basis whether or not a token that is sold in advance of a product launch embodies an investment component (pre-sales are highly relevant in the crowdfunding context). Furthermore, there are ongoing evaluations if self-determined utility tokens, that can be used on one platform for more than one purpose (e.g. payment of fees, exchange into other tokens) are payment tokens issued within a limited network according to PSD 2 or EMD 2.

The cases are very different, a case-by-case assessment cannot be avoided. It would be important to harmonize the legal assessment and apply uniform standards (e.g.: Does it depend on the main feature(s)? What if a utility token can be exchanged for more than one utility - does this qualify the token as payment token?). Form a supervisory standpoint, guidance on the relevant criteria regarding the legal assessment would be vital to achieve a harmonised approach in the classification of hybrid token.

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.

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

Completely agree	
Rather agree	X
Neutral	
Rather disagree	
Completely disagree	

Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

In principle, the provisions of the MiFID II- regime with regard to conduct of business and organizational requirements for investment firms are technology-neutral. The primary focus must be on whether a product (crypto asset) qualifies as a financial instrument according to MiFID II and whether a corresponding investment service is provided.
The corresponding technology-neutral wording of the relevant provisions leads to the applicability on business models that can be assigned to the FinTech sector which for example provide their investment services on a fully digital basis or even automatically and without human interaction (for example in the area of Robo Advice). Consequently, companies that provide investment services in relation to crypto assets that qualify as financial instruments would also be covered by these provisions and would be obliged to comply with the corresponding organisational and behavioural rules.

However, problems arise in the area of market infrastructure regulation (especially in the context of post-trade settlement) when operating MiFID-trading venues in connection with security token / blockchain-based financial instruments. These are discussed hereinafter in the context of the relevant questions.

63) **Do you think that a clarification or a guidance on applicability of such rules and requirements would be appropriate for the market?** [Insert text box]

Completely appropriate	X
Rather appropriate	
Neutral	
Rather appropriate	
Completely inappropriate	
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

Appropriate regulatory guidance at the European level would be of the utmost importance for both market participants and supervisory authorities, in order to ensure a harmonized approach in this area and to prevent further fragmentation through national solo efforts as well as to address potential risk areas and to contain them.

Accordingly, considerations regarding the creation of a bespoke regime on crypto assets / a regulatory framework for Blockchain / DLT would be important. If the investigations reveal insurmountable barriers between the current legal regulations and the technological design of the blockchain or DLT-systems, legal clarity through a new regulatory regime could maximize the full potential of this technology in the financial sector.

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.

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

Completely appropriate	
Rather appropriate	
Neutral	
Rather inappropriate	X
Completely inappropriate	
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

The FMA currently sees insurmountable regulatory obstacles when it comes to trading security token on MiFID-trading venues (See therefor the answer to question 66 below).

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 (if needed). [Insert text box]

Please explain your reasoning (if needed). [Insert text box]

The transposition of MiFID II into Austrian law or existing market practice in Austria neither facilitate nor prevent the use of DLT for investment services and activities. As already mentioned before, problems arise in the area of the market infrastructure regulation (see the following responses below).

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[57], platforms which would engage in trading of security tokens may fall under three main broad categories as follows:

[57] ESMA, 'Advice on Initial Coin Offerings and Crypto-Assets', January 2019

- 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[58].

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 (if needed).** [Insert text box]

[58] Recital 8 of MiFIR.

The FMA currently sees insurmountable regulatory obstacles if trading platforms for crypto assets, which could be qualified as trading venues in the sense of MiFID II regarding their functionality, list security token (i.e. DLT-based financial instruments):

The CSDR [Art 3 (2)] states that where a transaction in transferable securities takes place on a trading venue the relevant securities shall be recorded in book-entry form in a CSD on or before the intended settlement date, unless they have already been recorded. This securities account is defined as an account on which securities may be credited or debited. In principle, the CSDR does not impose one particular method for the initial book-entry recording. However, it states that the book-entry recording should be able to take the form of immobilisation or of immediate dematerialisation.

„Immobilisation" means the act of concentrating the location of physical securities in a CSD in a way that enables subsequent transfers to be made by book entry. „Dematerialised form" means that financial instruments exist only as book entry record. In any case, these book-entry recordings must take place at a CSD and therefore at a central location in the settlement process.

The obvious legal obstacle for trading security token, which are decentrally stored as transaction data on a Blockchain / in a DLT-system, are primarily in relation to the legally required forms of book-entry recording within a CSD. Completely decentralized systems such as the Ethereum blockchain, which acts as the basis for most security token according to the ERC 20 standard, by definition do not allow central entities in the network. A corresponding adaptation of common DLT-systems would run counter to the basic idea of such networks based on the idea of complete decentralisation.

The securities settlement systems covered by the CSDR are specified in the Directive 98/26/EC. However, such systems must be operated by a central organization, which also acts as the licensed entity. These considerations also result in the fact that trading platforms on which security token can be traded, cannot themselves be approved as CSDs and thus as operators of a securities delivery and settlement system, since they do not carry out the transactions themselves, but the network. This applies regardless of the design of the trading platform (in relation to on- or off-chain trading), since a transaction in a DLT network ultimately only becomes effective if it is confirmed via decentralized consensus.

Due to multiple problems in the area of market infrastructure regulations, it would be worth considering introducing a new form of trading venue in relation to crypto assets / security tokens ('crypto trading facilities') to solve regulatory issues and to reflect the current market conditions. For example, direct participation on traditional trading venues is widely prohibited for retail customers – however, on crypto exchanges, these make up a large proportion of trading participants. This could lead to retail customers switching to trading venues located in third countries, where direct trading participation is possible without the interposition of an intermediary. Since no intermediary is required to store crypto assets, there is not necessarily a contact point with the European financial system.
Regarding areas such as investor protection but also location policy, these regulatory gaps seem to be problematic.

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.

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 (if needed).** [Insert text box]

Yes, the current scope of investor protection rules is generally appropriate.

The principle of technology neutral supervision dictates that a business model / crypto-asset that is categorized as a financial instrument should be treated like any other traditional financial instrument – regardless of technical implementation. Most investor protection rules also do not cause significant issues when applied to crypto-assets since they target regulated intermediaries and not issuers who may or may not be available. Issuers of security tokens come in four broad types:
(1) traditional actors of the financial markets who use tokenization to adapt / broaden their product universe,
(2) actors who willingly and knowingly enter the realm of the traditional financial markets,
(3) actors who unwittingly create an instrument that falls within the scope of financial markets supervision and
(4) actors who maliciously (try to) create instruments equivalent to traditional financial instruments, ignoring or circumventing financial markets law.

These groups have to be considered when evaluating investor protection rules. When investor protection is trusted to issuers groups 3 and especially 4 can and will cause issues for consumers. Consequently, strong emphasis should be placed on rules that apply to regulated intermediaries. Rules that rely on issuers (e.g. Prospectus Regulation) may have to be adapted / supplemented to account for these actors.

It should also be noted that offering services / products cross-border is a very prevalent and hard to control phenomenon in the crypto-space for national competent authorities. This may warrant a discussion on the role of the ESAs in supervision and especially as a repository for information for consumers.

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 (if needed).** [Insert text box]

No, the existing rules appear sufficient. Online marketing of financial services is already regulated although not fully harmonized – sectoral differences as well as Member State options exist. We do not see significant differences to existing business models regarding marketing that would warrant different rules for economically equivalent instruments. Regarding enforcement the international nature of crypto-business-models might however necessitate certain adaptations of the approach to supervision of such cross-border models.

Generally we have identified marketing via social media as a channel in which a large number of dubious offers – not only in connection with crypto assets - appear.

69) Would you see any particular issue (legal, operational,) in applying MiFID investor protection requirements to security tokens? Please explain your reasoning (if needed). [Insert text box]

No. Whitepapers are often intransparent and unclear, similar regulations should also be applied to crypto assets that are financial instruments under MiFID II.

Some issues arise due to the decentralized market structure in the Crypto-Space. The goal of any regulation should be to achieve the same level of investor protection for security CAs as for traditional financial instruments under the MiFID II.

1.) Unregulated issuers currently do not fall into the scope of MiFID II when they issue a security (unlike e.g. the prospectus regulation). This leads to the potential outcome that an EU entity issues e.g. a note to the public. This note is then traded by EU retail clients on easily accessible and established third country trading platforms. Neither party is subject to MiFID II despite the instrument having been issued in the EU. It is questionable whether such an outcome is in the interest of consumer protection since this process could easily be used to circumvent MiFID II rules entirely.

2.) Best execution requirements could prove to be problematic due to information deficits in the market.

3.) The role of smart contracts may need to be explored further, especially regarding the handling of client orders.

4.) In current market structure in the crypto-economy retail clients make up a large portion of the transactions on organized but unregulated crypto-exchanges. Security Tokens would have to be traded on regulated markets (most likely MTFs). Retail clients are currently prohibited from directly trading in such markets. This prohibition is opposed to the idea behind the tokenization of financial instruments. A discussion of this rule is therefore necessary.

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.

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 (if needed).** [Insert text box]

Trading on DLT networks could indeed create significant efficiency gains for SME Growth Markets such as operational improvements, enhanced transparency, cost and risk reduction as well as liquidity gains, which are especially important for SME Growth Markets, since they often lack the necessary liquidity. However, a thorough analysis of potential implications of accommodating DLT technology into the current regulatory framework is important to understand the unintended consequences that this technology might bring.

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[59] 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.

71) **Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed? Please explain your reasoning (if needed).** [Insert text box]

No. Creating a level playing field is important and therefore equal treatment (regardless of the specific technology used) needs to be ensured.

[59] 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)

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.

72) **Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed? Please explain your reasoning (if needed).** [Insert text box]

No. Creating a level playing field is important and therefore equal treatment (regardless of the specific technology used) needs to be ensured.

Under current regulation, Art. 3(2) CSD-R is a requirement for admission to trading venues, which is hard to fulfil in the context of security tokens. Furthermore, Commission Delegated Regulation (EU) 2017/568 supplementing Directive 2014/65/EU with regard to regulatory technical standards for the admission of financial instruments to trading on regulated markets requires transparent und reliable underlyings for admission of derivatives. It is questionable if these criteria can be met with DLT.

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.

73) **What are the risks and benefits of allowing direct access to trading venues to a broader base of clients? Please explain your reasoning (if needed).** [Insert text box]

Preliminary Remark: The term „direct acess“ should be used with care in order to not cause misinterpretations with reference to “direct electronic access” according to MiFID II (which is completely different).

As a baseline any deviation from MiFID II trading platform standards for security token trading platforms should be well founded. Usually the operation of a trading platform requires the establishment of a multitude of rules any participant should be capable of adhering to. Even for “direct electronic access” according to MiFID II (which is no real “direct access”) a certain minimum of professional and regulatory requirements have to be fulfilled – is seems unclear why there should be no need for such requirements in the case of security token trading platforms.

1.10. Pre and post-transparency requirements

MiFIR[60] 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[61] 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.

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

Completely agree	
Rather agree	X
Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

While we agree that similar transparency requirements should apply to economically similar products/tokens, it may indeed prove challenging to develop meaningful thresholds.

[60] In its Articles 3 to 11

[61] 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.

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 (if needed).** [Insert text box]

A prerequisite for a transparency system for security tokens would be a working transaction reporting system with common identifiers and classifications (e.g. CFI codes, ISINs) for crypto assets. Additionally it remains unclear how e.g. decentralized trading platforms with no identifiable platform operators are included in a transaction reporting system. In order to make a transparency system work all transactions in classified security tokens have to be automatically tracked, recorded and reported to a centralized competent authority. Thresholds can be computed from the received data.

1.11. Transaction reporting and obligations to maintain records

MiFIR[62] 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).

76) **Would you see any particular issue (legal, operational) in applying these requirement to security tokens which should be addressed? Please explain your reasoning (if needed).** [Insert text box]

No. Creating a level playing field is important and therefore equal treatment (regardless of the specific technology used) needs to be ensured.

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.

[62] In its Article 25 and 26

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[63] 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.

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?

Yes, the Austrian Supervisory Authorities are of the opinion that Article 8 of MAR provides enough flexibility in this respect.

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.

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?
[Insert text box]

[63] Under MiFID Article 4(1)(24) 'trading venue' means a regulated market (RM), a Multilateral Trading Facility (MTF) or an Organised Trading Facility (OTF')

Yes. Article 12(1) lit. a of MAR reads as follows: ‚For the purpose of this Regulation, market manipulation shall comprise the following activities:

(a) entering into a transaction, placing an order to trade or **any other behaviour** which […]'

This specific wording (‚**any other behaviour**' or ‚**behaviour**') is repeatedly used. Due to this wording the MAR provisions are flexible enough to be applied to ‚new' markets falling in the scope of MAR. Clarification could be given e.g. through a review of the examples named in paragraph 2 of Article 12, the indicators (paragraph 3, Annex I of MAR) and the Level II examples (Del. Reg. (EU) 2016/522).

79) Do you think that there is a particular risk that manipulative trading in cryptoassets which are not in the scope of MAR could affect the price or value of financial instruments covered by MAR? [Insert text box]

Yes. This risk is evident whenever there are instruments that have or are likely or intended to have an effect on the price or value of a financial instrument referred to in Article 2(1) of MAR.

3. Short Selling Regulation (SSR)

The Short Selling Regulation[64] (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[65], 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.

80) Have you detected any issues that would prevent effectively applying SSR to security tokens? Please rate each proposal from 1 to 5, 1 standing for "not a

[64] Short Selling Regulation (236/2012/EU)

[65] ESMA, 'Advice on Initial Coin Offerings and Crypto-Assets', January 2019

concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
transparency for significant net short positions			X			
restrictions on uncovered short selling			X			
competent authorities' power to apply temporary restrictions to short selling			X			
Other					X	

Please explain your reasoning (if needed). [Insert text box]

General concerns

Generally speaking we try to understand the technical possibilities to sell security tokens short. In our understanding the security tokens will be handled via DLT. One of the key concepts of DLT is the proof of ownership, meaning that you can only sell crypto assets when you can proof the be in possession of it. In our understanding this contradicts the intention of selling short, where we have doubts to this proof could be evidenced on the chain. In practice this transaction could only take place off the chain, which seems to not be relevant for the current survey.

Scope

Reg. 236/2012 (SSR) defines the scope in Art. 1(1) in combination with Art. 2(1)(a) as
(a) financial instruments listed in section C of Annex I of MIFID I (further related to Annex I Section C MiFID II), which are admitted to trading on a trading venue in the Union,
(b) derivatives referred to in points (4) to (10) of Section C of Annex I to MiFID I, that relate to a financial instrument in point (a) and
(c) debt instruments issued by a Member State or the Union and derivatives, that relate or are referenced to debt instruments issued by a Member State or the Union.

With respect to point (a) this scope is further narrowed by reference to “issued share capital” as defined in Art. 2(1)(h) and used throughout that Regulation.
So the first issue when applying the SSR to security tokens is, that the scope and definitions need to be adapted in order to include such security tokens into the scope of SSR regime. As a foregoing step the classification of security tokens need to be made within MiFID II, as Section IV chapter A within this survey currently mentions security tokens as being “transferable securities or other types of MiFID financial instruments”.
As the definition in the scope of SSR refers to instruments admitted trading on a trading venue, this presupposes that those platforms, where security tokens are traded, are classified as Regulated Markets under MiFID II. Unless there is also a respective amendment within this part of the scope it is very unlikely that those security tokens would be brought under the SSR regime at all.

Identification

For the purpose of tracing the security token traded, it needs to have an ISIN assigned on a unique basis, and be part of the Financial Instruments Reference Data System (FIRDS). SSR exempts shares, which have a principal trading venue outside the Union. To perform those calculation NCA’s need to be in a position to compare traded volumes within the Union and outside the Union. Thus the provision of relevant turnover data is key.

RCA and notifications

In this context defining the relevant competent authority for the most liquid market in terms of liquidity (RCA) for security tokens needs to be also considered. The methodology for determining the RCA needs to be clarified accordingly within the MiFID II/ MiFIR provisions including the corresponding Technical Standards as notifications pursuant to Art. 5 SSR on net short positions need to be sent to the RCA of the financial instrument.

Temporary restrictions

One of the main drivers for consideration of temporary emergency measures under SSR is provided in Art. 23(1), which is a significant fall in the price of a financial instrument. As experience with crypto currencies showed is that those assets are regularly subject to high volatility. Before adapting the SSR framework it needs to be investigated if this driver would also apply for security tokens or if it is necessary to develop other criteria, which could trigger NCA’s to consider emergency measures.

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? [Insert text box]

No.

4. Prospectus Regulation (PR)

The Prospectus Regulation[66] 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.

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	x
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

We see no reasons for different or additional exemptions for security tokens other than the ones laid down in Article 1 (4) and Article 1 (5) of the PR.

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.

[66] Prospectus Regulation (2017/1129/EU)

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 nonequity 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[67] 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.

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

- **Yes**
- ~~**No**~~
- ~~**Don't know/no opinion**~~

If yes, 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

We are of the opinion that the building block approach is the most effective approach in this context. Specific additional information should be integrated in the existing schedules to provide a true and fair overview for potential investors. Such information should i.a. be:

- Rights attached to the security token
- Discretion rights of the issuer of the security token
- Functions of the security token
- Underlying crypto-assets
- Underlying technology.

[67] ESMA, Guidelines on Risks factors under the prospectus regulation (31-62-1293)

reasoning (if needed). [Insert text box]

84) **Do you identify any issues in obtaining an ISIN for the purpose of issuing a security token?** [Insert text box]

We did not identify any issues in obtaining an ISIN for the purpose of issuing a security token in Austria in connection with a public offer and a respective approved prospectus. In fact, in Austria issuers already have obtained an ISIN for a security token in the past.

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 (if needed).** [Insert text box]

We did not scrutinize special types of prospectuses or related documents under the PR to this date, therefore we could not identify any difficulties in practice regarding this 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**~~

Please explain your reasoning (if needed). [Insert text box]

Currently we do not see any reason for the introduction of an *ad hoc* alleviated prospectus type or regime for security tokens. Precisely in applying new technologies the focus should be on providing true and fair, hence comprehensive information. It is important that a level playing field between existing and new innovative business models is achieved. Any type of regulation in this regard has to be risk-based and proportionate.

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

Completely agree	X
Rather agree	

Neutral	
Rather disagree	
Completely disagree	
Don't know / No opinion	

If you agree, please indicate if ESMA's guidelines on risks factors should be amended accordingly. Please explain your reasoning (if needed). [Insert text box]

We completely agree that issuers of security tokens should disclose specific risk factors relating to the use of DLT. In fact, in the past we already required issuers to inter alia include „Risks specific to the tokenized Participation Rights" and „Risks specific to the Blockchain Technology" in security token – prospectuses.

5. Central Securities Depositories Regulation (CSDR)

CSDR[68] 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.

88) Would you see any particular issue (legal, operational, technical) with applying the following definitions in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern"

	1	2	3	4	5	No opinion

[68] Central Securities Depositories Regulation (909/2014/EU)

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

Please explain your reasoning. [Insert text box]

Regarding the problem areas arising in the field of CSDR (definition CSD; definition of book-entry form and dematerialised form) and SFD (definition securities settlement system), see the answer to question 66.

Records on a DLT platform could not be qualified as securities accounts within the meaning of Art 2 (28) CSDR, since these accounts are managed centrally by a CSD. However, records in a DLT system are kept decentralized as well as confirmed within a decentralized consensus mechanism. Whether wallets managed by a CSD can be qualified as securities accounts within the meaning of Art 2 (28) CSDR is a question that needs to be further discussed.

Regarding the definition of ‘settlement‘ within the meaning of Art 2 (7) CSDR, it should be kept in mind that the transaction processing within the framework of DLT systems deviates entirely from the traditional capital market area, since intermediaries have been completely eliminated and replaced by the decentralized consensus mechanism. In the context of DLT systems, the fact that transactions are concluded through the transfer of crypto assets and not through the transfer of FIAT currencies ('cash') also differs.

Since the transaction processing within (established) DLT systems (e.g. such as the Ethereum network) takes place through a decentralized consensus mechanism, no central entities as 'settlement internaliser' within the meaning of Art 2 (11) CSDR could be integrated into such a system,

“Delivery versus payment” (DVP) mechanisms are also established in the context of DLT systems. The systems counteract the potential danger of double spending (risk that a digital currency can be spent twice) with transaction verifications in the context of blockchains to verify the authenticity of each transaction and prevent double-counting. As part of this, the network uses the decentralized consensus mechanism to ensure that assets are only transferred if they actually exist and have not already been issued.

The development of smart contracts (e.g. in the area of the Ethereum network) ensures, for example within the framework of ICOs / ITOs / STOs, that as soon as a payment has been registered by the smart contract, the transfer process of the asset (token) is automatically initiated to the payer's wallet address.

However, it should be noted that in principle all payment processes (except the purchase of crypto assets against FIAT currencies) in the DLT / blockchain area are primarily concluded through crypto assets and are therefore not 100% compatible with the DVP-provisions in the sense of the CSDR (‘‘*links a transfer of securities with a transfer of cash*‘‘).

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

- ~~Yes~~
- **No**
- ~~Don't know/no opinion~~

Please explain your reasoning. [Insert text box]

No, as these book entries would have to take place within a central entity (CSD) which is incompatible compared to record keeping within a DLT system (see answer to question 66).

CSD Regulation requires the Issuer (also of security tokens) to arrange that the securities should be presented in „book-entry form as immobilisation or subsequent to a direct issuance in a dematerialised form“. Security Tokens are issued in a „dematerialised form“, however, under current Regulation, they would still need to be presented to the CSD to hold in „book-entry“ form. Theoretically as security tokens on a blockchain (DLT) are, in principle, in a „book-entry“ form *when combined* with a software application to monitor *the change of ownership*, it may conceive that CSDs may elect to accept the „book-entry“ system presented by the Issuer subject to the CSD being satisfied that that system meets its own requirements under CSD Regulations. However, the adoption of an *external* „book-entry“ system by the trading venue would only be of less interest to a trading venue. For centralised trading venues in security tokens, CSDR is relevant and they would need themselves to receive authorisation directly for that activity or cooperate with an already authorised CSD.

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.
[Insert text box]

Austrian law does currently neither prevent nor facilitate the use of DLT solution. But particularly worth mentioning is that although a public offer of security tokens is possible in Austria, a listing of securities in the form of security tokens isn’t possible under current legislation.

91) Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system					X	
Rules on measures to prevent settlement fails					X	
Organisational requirements for CSDs					X	
Rules on outsourcing of services or activities to a third party					X	
Rules on communication procedures with market participants and other market infrastructures					X	

Rules on the protection of securities of participants and those of their clients					X	
Rules regarding the integrity of the issue and appropriate reconciliation measures					X	
Rules on cash settlement					X	
Rules on requirements for participation					X	
Rules on requirements for CSD links					X	
Rules on access between CSDs and access between a CSD and another market infrastructure					X	
Other (including other provisions of CSDR, national rules applying the EU acquis, supervisory practices, interpretation, applications...)						

Please explain your reasoning (if needed). [Insert text box]

Rules on settlement periods and on measures to prevent settlement fails are defined in Art 6 and Art 7 CSDR. However, it is unclear how they should be implemented in DLT environment. Also the current rules on cash settlement are not plausible with DLT-possibilities as, in principle, all payment processes are primarily conducted through crypto assets (see question 88). Furthermore, the securities settlement systems operated by CSDs serve as an essential tool to control the integrity of an issue, hindering the undue creation or reduction of issued securities, and thereby play an important role in maintaining investor confidence. In order to ensure that, it would be necessary to set a mechanism or set of rules to ensure that in DLT environment as well. According Art 33 CSDR, for each securities settlement system it operates a CSD shall have publicly disclosed criteria for participation which allow fair and open access for all legal persons that intend to become participants. Such criteria shall be transparent, objective, and non-discriminatory so as to ensure fair and open access to the CSD with due regard to risks to financial stability and the orderliness of markets. Criteria that restrict access shall be permitted only to the extent that their objective is to justifiably control a specified risk for the CSD. Other rules and requirements are not currently applicable for DLT and need to be specified.

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[69]? Please explain your reasoning. [Insert text box]

No.

6. Settlement Finality Directive (SFD)

The Settlement Finality Directive[70] lays down rules to minimise risks related to transfers and

[69] Such as the requirements regarding the recording on an account with a custody account keeper outside a DLT environment

[70] Settlement Finality Directive (98/26/EC)

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.

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 each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
definition of a securities settlement system		x				
definition of system operator		x				
definition of participant		x				
definition of institution		x				
definition of transfer order			x			
what could constitute a settlement account			x			
what could constitute collateral security					x	
Other						

Please explain your reasoning. [Insert text box]

European guidance is needed to apply consistent legal interpretation of Union law throughout the EU.

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[71]? Please explain your reasoning. [Insert text box]

The applicable law for the system has to be defined by the operator according to the SFD. In the context of collateralization, the applicable law on registers needs to be clearly defined.

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? [Insert text box]

For conflicts of law, the Rome I Regulation (EC 593/2008) applies.

96) Do you consider that the effective functioning and/or use of DLT solution is limited

[71] 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.

or constrained by any of the SFD provisions?

- ~~**Yes**~~
- **No**
- ~~**Don't know/no opinion**~~

If yes, please provide specific examples (e.g. provisions national legislation transposing or implementing SFD, supervisory practices, interpretation, application...). Please explain your reasoning. [Insert text box]

7. Financial Collateral Directive (FCD)

The Financial Collateral Directive[72] 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[73].

97) Would you see any particular issue (legal, operational, technical) with applying

	1	2	3	4	5	No opinion
if crypto-assets qualify as assets that can be subject to financial collateral arrangements as defined in the FCD						x
if crypto-assets qualify as book-entry securities collateral						x

the following definitions in the FCD or its transpositions into national law in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

if records on a DLT qualify as relevant account						x
Other						

[72] Financial Collateral Directive (2002/47/EC)

[73] 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)

Please explain your reasoning. [Insert text box]

98) **FCD sets out rules on conflict of laws. Would you see any particular issue with applying these rules in a DLT network[74] ?** [Insert text box]

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?** [Insert text box]

100) **Do you consider that the effective functioning and/or use of a DLT solution is limited or constrained by any of the FCD provisions?**
- **Yes**
- **No**
- **Don't know/no opinion**

If yes, please provide specific examples (e.g. provisions national legislation transposing or implementing FCD, supervisory practices, interpretation, application...). Please explain your reasoning. [Insert text box]

8. European Markets Infrastructure Regulation (EMIR)

The European Markets Infrastructure Regulation (EMIR)[75] 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

[74] in particular with regard to the question according to which criteria the location of the account should be determined and thus which country would be considered the country in which the register or account, where the relevant entries are made, is maintained

[75] European Markets Infrastructure Regulation (648/2012/EU)

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.

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

Completely appropriate	
Rather appropriate	X
Neutral	
Rather inappropriate	
Completely inappropriate	
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

Technically they are. Generally, in the past a number of security token projects have begun to start working on this new business despite the uncertain regulatory climate. Not only in Europe, but worldwide, there are already several security token trading platforms in place. These are trading, clearing and settlement platforms for alternative assets like security tokens, which combine a centralized matching, clearing and settlement process.
However, new technologies, Fin-Techs and DLT are currently affecting also the financial system - worldwide. This is also affecting clearing. But we have to keep in mind that new technologies like central clearing for security tokens should fullfill the same rules and requirements as they are for other financial instruments. As a consequence, CCPs that are willing to offer those new services, need clear legal bases for their activities, governance structures that support their operations and sound risk management systems. At present, there is no European legal framework to ensure clarity and transparency within clearing of security tokens. For this reason, it is very welcomed to work on the implementation of a harmonised framework on this.

102) Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
Rules on margin requirements, collateral requirements and requirements regarding the CCP's investment policy			X			
Rules on settlement				X		
Organisational requirements for CCPs and for TRs			X			
Rules on segregation and portability of clearing members' and clients' assets and positions			X			
Rules on requirements for participation			X			
Reporting requirements			X			
Other (including other provisions of EMIR, national rules applying the EU acquis, supervisory practices, interpretation, applications...)						X

Please explain your reasoning (if needed). [Insert text box]

Platforms, CCPs and Customers and all projects dealing with those new technologies generally need a clear, transparent, and enforceable legal basis for each material aspect of their activities relating to DLT business. It is essential that there is a common understanding and definition of the term security token or crypto-asset. A proper legal definition is needed to define and understand what instruments qualify and what instruments do not qualify as such. This definition should be on a global base and this is important because different types of tokens or crypto assets are treated differently from an operational and a regulatory perspective. Currently there is no harmonised legally recognized classification of tokens on European level. Once there is a harmonised definition for security tokens including their characteristics, the next step should be to provide clear European guidance on how security token interact with the requirements of the relevant regulations.

Furthermore, we have concerns relating to the EMIR requirement of settlement in central bank money. Since there has been no official E-Euro introduction as of yet, there is also no established and viable solution for settlement in central bank money via DLT, at the moment.

103) Would you see the need to clarify that DLT solutions including permissioned blockchain can be used within CCPs or TRs? [Insert text box]

DLT solutions have the potential to provide a clear added value in terms of transparency and efficiency with regards to clearing and settlements activities. This means with this technology there is the possibility to cut out intermediate steps in these transactions chains altogether. Trades executed with blockchain technology remove the need for post-trade confirmation with central clearing due to the increased transparency. Transactions would take place near real-time. The challenge is within the usage of these new technologies is, that DLT solutions have to comply with existing requirements from the relevant European regulations like Prospectus, CSDR or EMIR. So, DLT solutions could be used within CCPs and Trade Repositoris (TR), but it will only have a sustainable presence in the industry, if they are underpinned by a stable, harmonised regulatory framework. At the moment such a framework is missing and without regulation those new technologies could face significant risks related to cyber-attacks, fraud or money laundering. In addition, within the usage of blockchain technology it should be clear who is in charge of what and who bears the liability. In the current clearing and reporting landscape there is the CCP or the TR who is responsible for the services offered. Within a DLT solution, those liabilities should be well defined as well.

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 (if needed). [insert text box]

As stated above the main issue is to fit the new technologies into the existing regulations. Therefore proper definitions for crypto assets are needed to understand their characteristics and to treat them under the relevant requirements from existing regulations. In addition the regulatory frameworks have to be updated or adapted to reflect the new technologies in the market. The difficulty may be that many EU jurisdictions (like Austria) follow a case by case assessment of the regulatory framework. This means that there is no general rule for crypto asset initiatives but competent authorities conduct a review in line with existing regulatory requirements for each initiative or project. For this reason, the experiences should be brought together and a harmonised regulatory framework. Consequently, it should be clear, that an EU-wide approach to regulation in this area is preferable to a country-by-country approach as described above. A coherent and coordinated approach at EU level will help to provide certainty and facilitate cross-border scaling opportunities, and should help combating regulatory arbitrage.

9. The Alternative Investment Fund Directive

The Alternative Investment Fund Managers Directive[76] (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 'security 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.

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 each proposal from 1 to 5, 1 standing for "not suited" and 5 for "very suited".

	1	2	3	4	5	No opinion
AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;	X					

[76] Alternative Investment Fund Managers Directive (2011/61/EU)

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

Please explain your reasoning (if needed). [Insert text box]

The questions is, whether crypto-assets can be entrusted to a depositary or not. In the first case, amendments within the AIFMD are necessary because crypto-assets would be in the scope of the AIFMD. In the latter case, the current provisions seem to be sufficient so far.

Considering the existing EU acquis, the Austrian Supervisory Authorities are of the opinion that crypto-assets can be entrusted to a depositary. That being said a European clarification in this regards would be needed to create legal certainty.

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**~~

If yes, please provide specific examples with relevant provisions in the EU acquis. Please explain your reasoning (if needed). [Insert text box]

Technical functionality of DLT-solutions is not impacted by the AIFMD.

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

The UCITS Directive[77] 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.

[77] Undertaking for Collective Investment in Transferable Securities Directive (2009/65/EC)

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.

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 each proposal from 1 to 5, 1 standing for "not suited" and 5 for "very suited".

	1	2	3	4	5	No opinion
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”				X		
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;				x		
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;				x		
UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;	x					
Disclosure and reporting requirements set out in the UCITS Directive				x		
Other - Risk management				x		

Please explain your reasoning (if needed). [Insert text box]

The questions is, whether crypto-assets can be entrusted to a depositary or not. In the first case, amendments within the UCITS-D are necessary because crypto-assets would be in the scope of the UCITS-D. In the latter case, the current provisions seem to be sufficient so far.

Considering the existing EU acquis, the Austrian Supervisory Authorities are of the opinion that crypto-assets can be entrusted to a depositary. That being said a European clarification in this regards would be needed to create legal certainty.

11. Other final comments and questions as regards security 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.

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**

If yes, please explain the regulatory approach that you favour. Please explain your reasoning (if needed). [Insert text box]

Again, as already stated above, it would become questionable for what reason the EU acquis for financial markets has been established if it is now largely “waived”.

109) Which benefits and risks do you see in enabling trading or post-trading processes to develop on permissionless blockchains and decentralised platforms? [Insert text box]

As stated above it should be kept in mind that the whole concept of regulation has been based upon authorization and supervision – both of which require the applicant or supervised entity to be capable of operating, adjusting and governing the arrangements and systems used when providing their services. It seems unclear how regulatory concerns might be adressed with that regard in cases of decentralized and permissionless systems. One of the key requirements therefore should deal with the providers capability of performing (when needed also substantial) adaptations to the systems used when necessary – for instance when new technologies arise that make the present technical systems unsafe. It seems difficult to imagine how that could be achieved with permissionless and decentralized systems.

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.

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**

If yes, please identify the issues that should be addressed at EU level and the approach to address them. Please explain your reasoning (if needed). [Insert text box]

See Answer to Q 27: DLT seems to fit the role of a settlement system rather than that of a trading system. It seems unclear how the basic functions of a trading system (bringing together of interests in buying and selling,) with its typical requirements of efficient and close to realtime trading can be performed “on chain” (particularly when it’s proof of work based). As the basic term “ledger” suggests, this rather could serve transfer or custodian/safekeeping purposes.

From a regulatory perspective a separation between custodian/settlement services (via DLT) and the operation of a trading platform (via centralized systems “off chain”) could possibly foster an orderly trading environment and therefore should be considered as part of regulation.

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? [Insert text box]

- **Yes**
- **No**
- **Don't know/no opinion**

Please provide specific examples and explain your reasoning (if needed). [Insert text box]

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**~~

Please provide specific examples (national provisions, implementation of EU acquis, supervisory practice, interpretation, application...). Please explain your

reasoning (if needed). [Insert text box]

There are no national provisions in Austria that would constrain the effective functioning of DLT solutions or the use of security tokens. But particularly worth mentioning is that although a public offer of security tokens is possible in Austria, a listing of securities in the form of security tokens isn't possible under current legislation.

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)[78] sets out the rules for the business practices and supervision of emoney institutions.

In its advice on crypto-assets[79], 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[80] (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.

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**~~

[78] Electronic Money Directive (2009/110/EC)
[79] EBA report with advice for the European Commission on "crypto-assets", January 2019
[80] Payment Services Directive 2 (2015/2366/EU)

Please provide specific examples (EMD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application...). Please explain your reasoning (if needed). [Insert text box]

Currently we do not consider the EMD2 as posing any problem for the functioning of e-money tokens, since from our perspective in most cases they are not within the scope of the Directive. Tokens do not fulfil the legal conditions of the EMD2 (no payment of funds, no third party relationship, no corresponding right to a claim, no central issuing body).

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**

Please provide specific examples (PSD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application.). Please explain your reasoning (if needed). [Insert text box]

Currently we do not consider PSD2 as posing any problem for the functioning of e-money tokens, since from our perspective in most cases they are not within the scope of the Directive. A transaction of an e-money token in most cases does not constitute a payment transaction as defined in Article 4 no. 5 PSD2. Such a payment transaction must have the consequence of a legal means of payment (funds, Article 4 no. 25) being transmitted as a consequence.

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**~~

Please provide specific examples and explain your reasoning (if needed). [Insert text box]

Yes. EMD2 and PSD2 should explicitly state that not only legal means of payments (funds pursuant to Article 4 (25) PSD2) should be addressed, but also virtual currencies (cf. the 5th Anti Money Laundering Directive). This would therefore ensure that e-money tokens would in any case be captured by the scope of application of this Directive. Ultimately a case-by-case review could be omitted, accompanied by a corresponding legal clarity.

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 stablecoins") 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 stablecoin” arrangements that could pose systemic risks.

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 each proposal from 1 to 5, 1 standing for "completely inappropriate" and 5 for "completely appropriate").

	1	2	3	4	5	No opinion
Initial capital and ongoing funds			X			
Safeguarding requirements	X					
Issuance	X					
Redeemability	X					
Use of agents			X			
Out of court complaint and redress procedures	X					
Other						

Please explain your reasoning (if needed). [Insert text box]

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 appropriate	
Rather appropriate	
Neutral	X
Rather inappropriate	
Completely inappropriate	
Don't know / No opinion	

Please explain your reasoning (if needed). [Insert text box]

Currently most payment token do not qualify as e-money and are therefore not within the scope of EMD 2 (e.g. lack of a central issuing body or rights to a claim). Because of that, first-hand experience with applying EMD 2 and PSD 2 to payment token is scarce. The Austrian Supervisory Authorities do take a neutral stance regarding the application of PSD 2 to stablecoins considering the currently available information.

Abbreviations

AIF - Alternative Investment Fund

AIFM - Alternative Investment Fund Manager

AIFMD - Alternative Investment Fund Managers Directive (2011/61/EU)

AML/CFT - Anti-Money Laundering/ Combatting the Financing of Terrorism AMLD5 - 5th Anti-Money Laundering Directive (Directive 2018/843/EU)

BCBS - Basel Committee on Banking Supervision

CCP - Central Clearing Counterparty

CDS - Credit Default Swap

CSD - Central Securities Depositories

CSDR - Central Securities Depositories Regulation (909/2014/EU)

DGSD - Deposit Guarantee Schemes Directive (2014/49/EU)

DLT - Distributed Ledger Technology

DMD - Distance Marketing of Consumer Financial Services Directive (2002/65/EC) EBA - European Banking Authority

ECB - European Central Bank

EIOPA - European Insurance and Occupational Pensions Authority

EMD2 - Electronic Money Directive (2009/110/EC)

EMIR - European Markets Infrastructure Regulation (648/2012/EU)

ESAs - European Supervisory Authorities (EBA, EIOPA, ESMA)

ESCB - European System of Central Banks

ESMA - European Securities Market Authority

ETF- Exchange-Traded Fund

EU- European Union

FATF - Financial Action Task Force

FCD - Financial Collateral Directive (2002/47/EC)

FSB - Financial Stability Board

ICO - Initial Coin Offering

ICT - Information Communication Technologies

IPO - Initial Public Offering

ISIN - International Securities Identification Number

LEI - Legal Entity Identifier

MAR - Market Abuse Regulation (596/2014/EU)

MiFIR - Markets in Financial Instruments Regulation (600/2014/EU)

MiFID II - Markets in Financial Instruments Directive II (2014/65/EU)

MTF - Multilateral Trading Facility

NCA - National Competent Authority

OTC - Over the Counter

OTF - Organised Trading Facility

P2P - Peer-to-peer

PSD 2 - Payment Services Directive 2 (2015/2366/EU)

PR - Prospectus Regulation (2017/1129/EU)

RM - Regulated Market

SFD - Settlement Finality Directive (98/26/EC)

SME - Small Medium Enterprise

STO - Security Token Offering

SSR - Short Selling Regulation (236/2012/EU)

TR - T rade Repository

UCITS - Undertaking for Collective Investment in Transferable Securities

UCITS Directive - Undertaking for Collective Investment in Transferable Securities Directive (2009/65/EC)

VASP - Virtual Asset Service Provider (as defined by the FATF)

Definitions

Blockchain: A form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerised process by which transactions are validated.

Crypto-asset: For the purpose of the consultation, a crypto-asset is defined as a type of digital asset that may depend on cryptography and exists on a distributed ledger.

Cryptography: the conversion of data into private code using encryption algorithms, typically for transmission over a public network.

Distributed Ledger Technology (DLT): means of saving information through a distributed ledger, i.e., a repeated digital copy of data available at multiple locations. DLT is built upon public-key cryptography, a cryptographic 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.

Financial instrument: those instruments specified in Section C of Annex I in MiFID II

Electronic money (e-money): '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 as defined in point 5 of Article 4 of

Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer;

E-money token: For the purpose of the consultation, e-money tokens are a type of cryptoassets that qualify as electronic money under EMD2.

Eurosystem: The Eurosystem comprises the ECB and the National Central Banks of EU Member States that have adopted the euro.

Global stablecoins: For the purpose of the consultation, a "global stablecoin" is considered as a "stablecoin" that is backed by a reserve of real assets and that can be accepted by large networks of customers and merchants and hence reach global scale.

Initial coin offering (ICO): an operation through which companies, entrepreneurs, developers or other promoters raise capital for their projects in exchange for crypto-assets (often referred to as 'digital tokens' or 'coins'), that they create.

Investment tokens: For the purpose of the consultation, investment tokens are a type of crypto assets with profit-rights attached to it.

Mining: a means to create new crypto-assets, often through a mathematical process by which transactions are verified and added to the distributed ledger.

Payment tokens: For the purpose of the consultation, payment tokens are a type of crypto-assets that may serve as a means of payment or exchange.

Permission-based DLT: a DLT network in which only those parties that meet certain requirements are entitled to participate to the validation and consensus process.

Permissionless DLT: a DLT network in which virtually anyone can become a participant in the validation and consensus process.

Utility tokens: For the purpose of the consultation, utility tokens are a type of crypto-assets that may enable access to a specific product or service.

Security tokens: For the purpose of the consultation, security tokens are a type of cryptoassets that qualify as a financial instruments under MiFID II.

Security token offering: an operation through which companies, entrepreneurs, developers or other promoters raise capital for their projects in exchange for 'security tokens' that they create.

Stablecoins: For the purpose of the consultation, "stablecoins" are considered as a form of payment tokens whose price is meant to remain stable through time. Those "stablecoins" are typically asset-backed by real assets or funds 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).

Trading venue: Under MiFID Article 4(1)(24), trading venue means a regulated market, a multilateral trading facility, or an organised trading facility (OTF').

Virtual Currencies: Under AMLD5, virtual currency means *'digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically'.*

Wallet provider: a firm that offers storage services to users of crypto-assets.