Contribution ID: 97e617d0-aa79-48fd-94f8-ec7661c31f48
Date: 19/03/2020 16:49:47

Public consultation an EU framework for markets in crypto-assets

Fields marked with * are mandatory.

Introduction

This consultation is also available in German and French.

Background for this public consultation

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

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

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

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

Crypto-assets are one of the major applications of blockchain for finance. Crypto-assets are commonly defined as a type of private assets that depend primarily on cryptography and distributed ledger technology as part of their inherent value[2]. For the purpose of this consultation, they will be defined as "a digital asset that may depend on cryptography and exists on a distributed ledger". Thousands of crypto-assets, with different features and serving different functions, have been issued since Bitcoin was launched in 2009[3]. There are many ways to classify the different types of crypto

assets[4]. A basic taxonomy of crypto-assets comprises three main categories: 'payment tokens' that may serve as a means of exchange or payment, 'investment tokens' that may have profit-rights attached to it and 'utility tokens' that may enable access to a specific product or service. The crypto-asset market is also a new field where different actors - such as the wallet providers that offer the secure storage of crypto-assets, exchanges and trading platforms that facilitate the transactions between participants – play a particular role

Crypto-assets have the potential to bring significant benefits to both market participants and consumers. For instance, initial coin offerings (ICOs) and security token offerings (STOs) allow for a cheaper, less burdensome and more inclusive way of financing for small and medium-sized companies (SMEs), by streamlining capital-raising processes and enhancing competition. The 'tokenisation' of traditional financial instruments is also expected to open up opportunities for efficiency improvements across the entire trade and post-trade value chain, contributing to more efficient risk management and pricing[5]. A number of promising pilots or use cases are being developed and tested by new or incumbent market participants across the EU. Provided that platforms based on Digital Ledger Technology (DLT) prove that they have the ability to handle large volumes of transactions, it could lead to a reduction in costs in the trading area and for post-trade processes. If the adequate investor protection measures are in place, crypto-assets could also represent a new asset class for EU citizens. Payment tokens could also present opportunities in terms of cheaper, faster and more efficient payments, by limiting the number of intermediaries.

Since the publication of the FinTech Action Plan in March 2018, the Commission has been closely looking at the opportunities and challenges raised by crypto-assets. In the FinTech Action Plan, the Commission mandated the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) to assess the applicability and suitability of the existing financial services regulatory framework to crypto-assets. The advice[6] received in January 2019 clearly pointed out that while some crypto-assets fall within the scope of EU legislation, effectively applying it to these assets is not always straightforward. Moreover, there are provisions in existing EU legislation that may inhibit the use of certain technologies, including DLT. At the same time, EBA and ESMA have pointed out that most crypto-assets are outside the scope of EU legislation and hence are not subject to provisions on consumer and investor protection and market integrity, among others. Finally, a number of Member States have recently legislated on issues related to crypto-assets which are currently not harmonised.

A relatively new subset of crypto-assets – the so-called "stablecoins" - has emerged and attracted the attention of both the public and regulators around the world. While the crypto-asset market remains modest in size and does not currently pose a threat to financial stability[7], this may change with the advent of "stablecoins", as they seek a wide adoption by consumers by incorporating features aimed at stabilising their 'price' (the value at which consumers can exchange their coins). As underlined by a recent G7 report[8], if those global "stablecoins" were to become accepted by large networks of customers and merchants, and hence reach global scale, they would raise additional challenges in terms of financial stability, monetary policy transmission and monetary sovereignty.

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

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

Responding to this consultation and follow up to the consultation

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

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

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

- **The second section seeks feedback from stakeholders on whether and how to classify crypto-assets**. This section concerns both crypto-assets that fall under existing EU legislation (those that qualify as 'financial instruments' under MiFID II and those qualifying as 'e-money' under EMD2) and those that do not.
- **The third section invites views on the latter, i.e. crypto-assets that currently fall outside the scope of the EU financial services legislation. In that first section, the term 'crypto-assets' is used to designate all the crypto-assets that are not regulated at EU level[12]. At certain point in that part, the public consultation makes further distinction among those crypto-assets and uses the terms 'payment tokens', "stablecoins" 'utility tokens', 'investment tokens'.**. The aim of these questions is to determine whether an EU regulatory framework for those crypto-assets is needed. The replies will also help identify the main risks raised by unregulated crypto-assets and specific services relating to those assets, as well as the priorities for policy actions.
- **The fourth section seeks views of stakeholders on crypto-assets that currently fall within the scope of EU legislation, i.e. those that qualify as 'financial instruments' under MiFID II and those qualifying as 'e-money' under EMD2. In that section and for the purpose of the consultation, those regulated crypto-assets are respectively called 'security tokens' and 'e-money tokens'**. Responses will allow the Commission to assess the impact of possible changes to EU legislation (such as the Prospectus Regulation , MiFID II, the Central Security Depositaries Regulation, ...) on the basis of a preliminary screening and assessment carried out by the Commission services. This section is therefore narrowly framed around a number of well-defined issues related to specific pieces of EU legislation. Stakeholders are also invited to highlight any further regulatory impediments to the use of DLT in the financial services.

To facilitate the reading of this document, a glossary and definitions of the terms used is available at the end.

The outcome of this public consultation should provide a basis for concrete and coherent action, by way of a legislative action if required.

This consultation is open until 19 March 2020.

---

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

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

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

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

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

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

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

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

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

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

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

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

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

More information:

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

About you

* Language of my contribution

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

- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

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

* First name

[redacted]

* Surname

[redacted]

* Email (this won't be published)

[redacted]

* Country of origin

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

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

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

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

* Organisation name

255 character(s) maximum

Association pour le Développement des Actifs Numériques

* Organisation size

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

Transparency register number

255 character(s) maximum

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

600495937657-61

* Field of activity or sector (if applicable):

at least 1 choice(s)

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

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

- (•) Benchmark administrator
- ( ) Benchmark contributor
- ( ) Benchmark user
- ( ) Other

* Publication privacy settings

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

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

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

☑ I agree with the personal data protection provisions

I. Questions for the general public

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

Question 1. Have you ever held crypto-assets?

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

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

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

Question 3.1 Please explain the reasons why you are planning to hold crypto-assets:

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

> As a non-profit association advocating for the development of blockchain and crypto-assets industry, ADAN may in the future hold any crypto-assets.
>
> The reasons for holding crypto-assets as a non-profit association may be: accepting membership fees paid in cryptocurrencies or stablecoins, paying for services on blockchain-based applications, paying service providers that only accept crypto-assets as a means of payment, or investing excess treasury.

Question 4. If you do plan or expect to hold crypto-assets in the future, please explain in what timeframe?

- (●) in the coming year
- ( ) 2-3 years
- ( ) more than 3 years

II. Classification of crypto-assets

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

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

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

---

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

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

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

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

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

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

Yes.
The scope of this consultation should be limited to crypto-assets. Most arguments are based on the characteristics allowed by the underlying DLT, then could not be valid under other assumptions.
Our opinion is that "crypto-assets" are defined :
- through a technological angle (registered on a DLT), and
- by their general characteristics (a digital asset being purely digital, permanent, non-duplicable and directly apprehensible).

They can cover a very wide range of use cases. That is why defining "crypto-assets" with purely legal perspectives is not relevant as there one single regulatory regime will not be able to cover all the use cases.

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

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

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

Please explain your reasoning:

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

Yes.
The classification of crypto-assets should lay the foundations for their regulation. This means that the rationale behind the definition of one category of crypto-assets should be the existence or the necessary creation of its specific regulatory regime.
To this end, crypto-assets that qualify with existing legal instruments should not lead to the creation of other categories.
For crypto-assets that do not fit into any existing legal concepts, two qualifications should be created :
- "cryptocurrencies" for crypto-assets that are governed by the blockchain protocol itself,
- "tokens" or "(programmable) crypto-assets" for those which are issued by an identified person (or several) and whose main features are determined by the issuer(s).

A flexible framework should be built upon very granular requirements. The application of each provision would depend on:
- the technological features of the crypto-asset: cryptocurrency or programmable asset,
- its inherent characteristics (see General comments point b) above),
- the activity/services operated on such crypto-assets,
- a risk analysis of the combination of all these elements, that is comparing the risk profile of the actor with the guarantee that they provide regarding: financial stability, user protection, fair competition.

This approach seems pragmatic and close to the reality behind the great heterogeneity of crypto-assets. In our opinion, a classification based solely on economic considerations could not be the best option as it has already proved insufficient (hybrid tokens, evolving tokens, some tokens do not easily fit into one category). See answer to question 8.
"Crypto-assets" that do not qualify under existing legislation should then be analysed on a case-by-case basis and a bottom up logic. This should be the function of a new regulatory or self-regulatory body dedicated to crypto-asset markets.
Moreover, regarding the potential of crypto-assets for great and fast evolutions, coupled with the lack of history of this young ecosystem, new legal mechanisms should enable flexibility and possible fast changes, at least during the first years of this regime.

Question 7. What would be the features of such a classification?

When providing your answer, please indicate the classification of crypto-assets and the definitions of each type of crypto-assets in use in your jurisdiction (if applicable).

Please explain your reasoning:

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

Among those which do not qualify under any existing legal concept, the classification of crypto-assets should consider their technological foundation. That is why “cryptocurrencies” and “(programmable) crypto-assets”/” tokens” should be distinguished.

Then the activity/service provided on such crypto-assets, their intrinsic features and their risk profile should help define among a set of rules which regulatory requirements should apply.

As a point of reference, in France, crypto-assets are classified under the following two categories:
- Crypto-assets that qualify as “digital assets” under the new PACTE regime. “Digital assets” encompass both ICO “tokens” and “virtual currencies” defined in AMLD5. Based on the functional analysis described above, this would include cryptocurrencies and a wide range of programmable tokens.
Article L. 552-2 of the French Monetary and Financial Code defines a “token” as “any intangible asset representing, in digital form, one or more rights that can be issued, registered, stored or transferred by means of a shared electronic recording device making it possible to identify, directly or indirectly, the owner of said asset”

Art. L. 54-10-1 of the French Monetary and Financial Code defines “digital assets” as:
“1° The tokens mentioned in article L. 552-2, excluding those fulfilling the characteristics of the financial instruments mentioned in article L. 211-1 and the “bons de caisse” mentioned in article L. 223 -1;
2° A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically”

- Crypto-assets that do not qualify as “digital assets” under the new PACTE regime.
- This explicitly covers tokens that qualify as financial instruments (as established in the “digital assets” definition) and “bons de caisse” .
- This implicitly refers to any other crypto-assets that do not fit into the “digital assets” definition, such as for example non-fungible tokens and stablecoins.

The ADAN considers this legal classification as a good first step that needs to be further specified - notably with regards to non-fungible tokens or other edge cases.

Notwithstanding the inherent complexity of this variety of assets that can have significant consequences in terms of legal analysis, apprehension, taxation of profits, etc., it is very important to consider that most of those assets have a common ground of characteristics that justify a common regulation of the actors of the industry (similarly to the MiFiD regulation that covers actors dealing with all and every kind of financial instruments).

In consequence, we are in favor of a two-level legal analysis:
- A legal analysis and regime at the level of the assets, as described above, that would help categorize each and every assets based on their sets of characteristics;
- A legal analysis and regulatory regime at the level of the actors dealing with the crypto-assets in general, in order to ensure a significant level of professionalism, ethics and integrity in market practices, security, AML/FT procedures, etc - which corresponds to the definition and regulation of so-called « VASPs » as defined by the FATF or the « PSAN » in the French legislation.

Question 8. Do you agree that any EU classification of crypto-assets should make a distinction between ‘payment tokens’, ‘investment tokens’, ‘utility tokens’ and ‘hybrid tokens’?

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

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

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

The EU classification of crypto-assets should probably not bear on the traditional distinction between “payment tokens”, “investment tokens”, “utility tokens” and “hybrid tokens”.

As previously exposed, the EU classification of crypto-assets should distinguish crypto-assets that already qualify under one current legislation from others. Among others are “cryptocurrencies” and “tokens”/” (programmable) crypto-assets”. For them, an ad hoc regime should be created where underlying rules focus on the service/activity provided, the intrinsic characteristics of assets and their risk profile.

Moreover, the traditional categorisation shows some flaws:
- So-called “payment tokens” are usually not only used as means of payment - they can be used as collateral or as a store of value, generate interest under specific conditions and more generally be considered as a multi-purpose bearer asset (this is specifically the case for digital assets usually referred to as “cryptocurrencies” or “protocol tokens”) ;
- “Investment tokens” can be hard to differentiate from regulated securities and prompt regulatory arbitrage ;
- “Utility tokens” is a very broad concept that basically comes to “anything that is not a payment token nor a security”.

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

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

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

This question could be raised for one single crypto-asset category: fiat-collateralized stablecoins which would be issued under the request of clients and only against the counterparty of their payments. To date and to the best of our knowledge, such stablecoins do not exist.

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

This section aims to seek views from stakeholders on the opportunities and challenges raised by crypto-assets that currently fall outside the scope of EU financial services legislation[15] (**A.**) and on the risks presented by some service providers related to crypto-assets and the best way to mitigate them (**B.**). This section also raises horizontal questions concerning market integrity, Anti-Money laundering (AML) and Combatting the Financing of Terrorism (CFT), consumer /investor protection and the supervision and oversight of the crypto-assets sector (**C.**).

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

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

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

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

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

	1 (not important at all)	2	3	4	5 (very important)	Don't know / no opinion / not relevant

Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs	○	○	○	◉	○	○
Issuance of utility tokens as an alternative funding source for start-ups	○	○	○	◉	○	○
Cheap, fast and swift payment instrument	○	○	○	○	◉	○
Enhanced financial inclusion	○	○	○	○	◉	○
Crypto-assets as a new investment opportunity for investors	○	○	○	○	◉	○
Improved transparency and traceability of transactions	○	○	○	○	◉	○
Enhanced innovation and competition	○	○	○	○	◉	○
Improved liquidity and tradability of tokenised 'assets'	○	○	○	◉	○	○
Enhanced operational resilience (including cyber resilience)	○	○	◉	○	○	○
Security and management of personal data	○	○	○	○	○	◉
Possibility of using tokenisation to coordinate social innovation or decentralised governance	○	○	○	○	◉	○

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

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

N/A

10.2 Please explain your reasoning for your answers to question 10:

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

All the aforementioned benefits brought by crypto-assets are important.

We would like to emphasise the importance of two opportunities:
- improved transparency and traceability of transactions is a very strong attribute of public blockchain-based use cases that can bring benefits to various transactions executed on blockchain at the stage of execution but also and especially after the execution stage. It has already been proved extremely useful to

audit blockchain-based application behaviours after bugs or exploitation, to monitor the evolution of a specific service, or to analyse major transaction flows that help better understand the structuring of blockchain-based use cases. As an example, a company like Alethio can use blockchain data to create useful visualisation of the interdependency of different blockchain products.

- using tokenization to coordinate social innovation or decentralized governance is at the exploration stage but some experiments are worth watching. As an example, the Tezos blockchain is self-amending, and improves its functionalities based on implementation of software upgrades that are voted by the token holders of the blockchain. Other examples include structures created at the application level of blockchains, such as DAOs. Those are usually created around a project, or a use case, and allow the participants to coordinate in order to realize the said project, e.g. MolochDAO that coordinates different players to fund the development of some elements of infrastructure of the Ethereum 2.0 protocol.

Despite the significant benefits of crypto assets, there are also important risks associated with them. For instance, ESMA underlined the risks that the unregulated crypto-assets pose to investor protection and market integrity. It identified the most significant risks as fraud, cyber-attacks, money-laundering and market manipulation[16]. Certain features of crypto-assets (for instance their accessibility online or their pseudo-anonymous nature) can also be attractive for tax evaders. More generally, the application of DLT might also pose challenges with respect to protection of personal data and competition[17]. Some operational risks, including cyber risks, can also arise from the underlying technology applied in crypto-asset transactions. In its advice, EBA also drew attention to the energy consumption entailed in some crypto-asset activities. Finally, while the crypto-asset market is still small and currently pose no material risks to financial stability[18], this might change in the future.

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

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

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

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

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

	1 (not important at all)	2	3	4	5 (very important)	Don't know / no opinion / not relevant
Fraudulent activities	○	◉	○	○	○	○
Market integrity (e.g. price, volume manipulation, ...)	○	○	◉	○	○	○
Investor/consumer protection	○	○	○	◉	○	○

Anti-money laundering and CFT issues	○	○	◉	○	○	○
Data protection issues	○	◉	○	○	○	○
Competition issues	○	◉	○	○	○	○
Cyber security and operational risks	○	○	○	◉	○	○
Taxation issues	○	◉	○	○	○	○
Energy consumption entailed in crypto-asset activities	○	◉	○	○	○	○
Financial stability	○	◉	○	○	○	○
Monetary sovereignty/monetary policy transmission	○	◉	○	○	○	○

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

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

N/A

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

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

Giving an absolute general score and comparing risks with others is quite difficult.

First, not all crypto-assets are homogeneous, and some can bear some risks that others do not. For example, risks related to monetary sovereignty and policy transmission are almost exclusively borne by “stablecoins”. Market integrity is not an issue within a private network. Energy consumption is highly dependent on the blockchain protocol used and more specifically its consensus protocol.

Second, risks depend on the activities/services provided on these crypto-assets. For instance, ML-FT risks are much weaker regarding crypto-crypto exchanges than crypto-fiat exchanges (see below). That is why a meaningful risk analysis requires a more granular case-by-case approach to better reflect the heterogeneity of crypto-assets.
“Fraudulent activities” is a very broad concept which can potentially refer to many various topics, that is why it seems difficult to appraise a general level of risk.

“Anti-money laundering and CFT issues” exist, but should not be overstated. AML-CFT issues have been analysed by the French Treasury in its national report on ML-FT risks published in september 2019. If they

observe that crypto-assets can (practically) be diverted from their right use in order to circumvent AML-CFT regulations, the French authority qualifies their risk score as “moderate” (on a scale from “weak” to “high”). Some of their arguments are:

- The illicit use of crypto-assets for ML-FT purposes is not a preferred option for criminals. These disincentives are the specific knowledge and a technical expertise that they require, and their volatility. That is why the French Treasury states that there are very few cases where crypto-assets are used for such illegal purposes. Crypto-crypto activities are less exposed to ML-FT threats as they do not imply re-injecting funds into the classical economic circuits.
- In a number of scenarios, information stored on-chain and off-chain by actors allow for the identification of clients and the tracking of transactions.
- The French legal framework for crypto-assets has been designed to mitigate the ML-FT risks with a logic of proportionality: the most concerned activities (crypto-custody and crypto-fiat exchanges) must comply with the AMLD5 whereas others can if they want to get a license from the French financial regulator.

The full report is available here, please refer to pages 64 to 67: https://www.economie.gouv.fr/files/files/directions_services/tracfin/analyse-nationale-des-risques-lcb-ft-en-France-septembre-2019.pdf

“Stablecoins” are a relatively new form of payment tokens whose price is meant to remain stable through time. Those “stablecoins” are typically asset-backed by real assets or funds (such as short-term government bonds, fiat currency, commodities, real estate, securities, ...) or by other crypto-assets. They can also take the form of algorithmic “stablecoins” (with algorithm being used as a way to stabilise volatility in the value of the coin). While some of these “stablecoins” can qualify as ‘financial instruments’ under MiFID II or as e-money under EMD2, others may fall outside the scope of EU regulation. A recent G7 report on ‘investigating the impact of global stablecoins’ analysed “stablecoins” backed by a reserve of real assets or funds, some of which being sponsored by large technology or financial firms with a large customer base. The report underlines that “stablecoins” that have the potential to reach a global scale (the so-called “global stablecoins”) are likely to raise additional challenges in terms of financial stability, monetary policy transmission and monetary sovereignty, among others. Users of “stablecoins” could in principle be exposed, among others, to liquidity risk (it may take time to cash in such a “stablecoin”), counterparty credit risk (issuer may default) and market risk (if assets held by issuer to back the “stablecoin” lose value).

Question 12. In our view, what are the benefits of ‘stablecoins’ and ‘global stablecoins’? Please explain your reasoning.

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

In recent years stablecoins have been seen as the opportunity to build the payment leg that blockchain applications lacked at the beginning. Contrary to cryptocurrencies such as bitcoin and ether, the stability of stablecoins makes them a more credible alternative as a means of payment. By guaranteeing users to redeem them at any time against legal tender currency, stablecoins could attract new consumers of blockchain-based products and services.

But perspectives around stablecoins go further than the crypto-asset ecosystem as they can improve the efficiency of traditional financial infrastructures from payment to settlement. In such context, they qualify as “wholesale stablecoins”, ie. for use by financial institutions and large companies,

Stablecoins are programmable “money”. Programmability and automation could optimise the delivery versus payment (DvP) of transactions. According to a decentralized model, crypto-assets and payment assets are usually entered into an “escrow smart contract” until the two players confirm that they agreed upon their

trading conditions. If such conditions are met, the smart contract automatically triggers the exchange of assets. Conversely, if the smart contract does not receive confirmation from the parties or contradictory information from the seller and the buyer, the smart contract does not execute the transaction and send back assets to each party (crypto-assets for the seller, the settlement asset for the buyer). That is why decentralized DvP requires both assets and means of payment to be “tokenized“ to ensure the atomic execution of transactions. Otherwise, if the cash leg is not managed on chain, DvP involves that the off chain “cash leg” and the on chain “crypto-asset” leg of transactions are executed simultaneously, which can be very complex to implement. Stablecoins could then allow to fully process transactions on blockchain.

Decentralized DvP and the full integration of transaction processing on blockchain are likely to provide higher liquidity to crypto-asset markets. Liquidity materializes through the growing participants attracted by stablecoins as a safe means of payment, their possible instantaneous redeemability, the higher speed of transaction processing, the cost economy that results from automation of processes, and the annihilation of counterparty risk.

“Retail stablecoins”, issued for individuals, could allow under- or even unbanked to overcome the difficulties encountered in order to transfer funds between individuals. Stablecoins fall within the growing trend of recent years to the digitization of cashless payments, led notably by Google, Apple, Facebook and Amazon. These new means of payment, which can be easily used with a mobile phone, support greater financial inclusion for populations where the banking system and payment infrastructures are the least efficient (or even do not exist). Today 1.7 billion adults are unbanked but 1.1 billion have a mobile phone (two thirds of them) and, in developing economies, 44% of adults use digital payments . In addition, the programmability of those assets would allow for the use of blockchain-based applications with high levels of security, reliability, auditability and transparency.

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

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

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

Data protection issues	○	○	○	◉	○	○
Competition issues	◉	○	○	○	○	○
Cyber security and operational risks	○	○	◉	○	○	○
Taxation issues	◉	○	○	○	○	○
Energy consumption	◉	○	○	○	○	○
Financial stability	○	○	◉	○	○	○
Monetary sovereignty/monetary policy transmission	○	○	○	◉	○	○

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

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

N/A

13.2 Please explain in your answer potential differences in terms of risks between "stablecoins" and 'global stablecoins':

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

First of all, it should be noted that all stablecoins are likely to qualify as "global stablecoins" (under the G7 Stablecoins Task Force's definition) at some point in time. Most stablecoins are actually designed to be used by the largest scope of people. Current operational stablecoins - such as DAI, Tether, USDC, etc. - have actually achieved a global scale. Therefore no difference should be made in a regulatory perspective or risk-based approach.

Rather than comparing stablecoins and global stablecoins, a more relevant distinction when appraising their potential risks and regulation framework could be their underlying stabilization mechanisms. Current analyses worldwide (G7, IOSCO, ECB, etc.) focus on fiat-collateralized stablecoins only. However it is likely that collateralized and non-collateralized/algorithmic stablecoins do not involve the same risks. Even within collateralized stablecoins, differences could arise from the nature of assets that back stablecoins.

For example, one risk that is not mentioned here is that for fiat-collateralized stablecoins, the collateral management must be operated by regulated credit institutions. The current negative rate environment makes such activity quite difficult from an economic perspective.

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

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

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

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

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

A bespoke regime for crypto-assets (that are not currently covered by EU financial services legislation) is crucial to enable a sustainable crypto-asset ecosystem in the EU. Legal uncertainty is detrimental to the long-term vision of business then prevents from the broad adoption of crypto-assets. This is also the opportunity for the EU to set a clear and favourable regulatory land where Asia and North America have not taken the lead yet.
But this regime should meet some essential conditions to be able to inspire confidence for users and business partners with the crypto industry while allowing actors to foster their innovative potential. To this end, proportionality, efforts to move away from traditional regulations that can inspire regulatory works, and granularity in determining roles and responsibilities of new actors are critical.

Moreover, an EU regime for crypto-assets must be really unified among Members. National initiatives to clarify the regulatory treatment of crypto-assets can be lauded but raise risks in terms of regulatory arbitrage between Member states.

To be really efficient, a unified EU bespoke regime should not rely on a directive. As it is only giving objectives to State members that then develop their own national provisions to achieve them, experience has proven that national regulatory frameworks could diverge a lot among State members creating conditions for unfair competition and regulatory arbitrage. A regulation would be a preferred option as it is transposed into national laws directly.

An alternative to such legislative texts could be the creation of a "28th regime". Recital 14 of the Rome 1 Regulation allows for designing an "optional instrument" (or "28th regime") that would be a second regime "providing parties with an option between two regimes of domestic contract law" . According to article 3 of the Rome 1 Regulation, parties can choose the law by which their contract shall be governed. In this scenario, national regimes when there are (such as the French PACTE Law) could co-exist with an EU crypto-asset regime.

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

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

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

The French regulatory regime on crypto-assets

Promulgated on 22 May 2019, the “PACTE law” provides an innovative regulatory framework for some actors of the crypto-asset industry and their supervision by French financial regulators (AMF and ACPR). These actors are:

a) token issuers

b) digital asset service providers (“PSAN”).

a) The French Financial Markets Authority (AMF) can issue an “ICO” visa for an offering when the token issuer complies with some underlying requirements, mainly relating to the content of the white paper and promotional marketing materials, the monitoring and safeguarding of the assets (both legal money and crypto-assets) collected all along the ICO and anti-money laundering and counter-financing of terrorism. This visa is optional, meaning that token issuers are not prohibited to launch their ICO to the French public if they do not ask for the visa or do not obtain it. However, the visa provides some advantages. The most relevant one for actors today is the unrestricted access to banking services: they cannot be refused access by credit institutions to deposit and payment account services. For such a refusal, or if they did not answer to the actor’s request by 2 months, credit institutions must provide the AMF and the ACPR with the reasons for this refusal. The ACPR can offer actors the possibility to ask the French Central Bank for appointing one credit institution to provide required services.

Another advantage is that the visa can be perceived as a comparative competitive advantage. Indeed, the visa is likely to become one important element in the decision-making of potential token buyers. However, it is important to precise that the visa is only an approval granted by the AMF to certify that the token issuer comply with its underlying requirements. The AMF does not approve the appropriateness of the project, nor authenticate information, nor verify the smart contract. Moreover, when the AMF issues a visa, the white paper must remind potential token buyers of the risks arising from such operations through a “general warning notice”.

Aside from the visa regime, the French Financial Markets Authority has also launched since 2017 its UNICORN (Universal Node to ICO’s Research & Network) program to support blockchain project holders wishing to raise funds using an ICO, and to conduct research on these operations in order to develop their expertise and better understand the impact of ICOs on the real economy and their implication for the protection of both token issuers and holders.

b) In line with the new visa introduced by the AMF for the primary token market, the “PACTE law” aims at regulating the secondary market and peripheral services for subscribers of digital assets.

The PACTE law establishes a list of nine “services on digital assets”. While it is largely inspired by that of investment services subject to European financial market regulation, certain services - notably the custody of digital assets and the exchange of digital assets with other digital assets - are more original.

ADAN comments on the French regime

In our opinion, the French regime is a very good foundation.

- The choice for optionality shows that French regulators understand that the crypto industry is not mature yet and needs simplicity and proportionality to structure itself. France has therefore taken the middle ground approach: on the one hand compulsory check of the AML rule for the “gatekeepers” (crypto-fiat exchanges and custodians) to address money laundering risks but, on the other hand, and at the same time optionality to get a full licence.
- The fact that credit institutions cannot refuse, without a strong motive, to open banking accounts to actors that got an ICO visa or are registered or authorized by the AMF is a powerful provision to overcome some cultural boundaries.

However, they might be some possible improvements:

- A clarification of the scope of some services on digital assets. For example, the category “exchange of digital assets” (with legal money or other digital assets) should explicitly exclude liquidity providers or people that distribute their token to allow their client to access their services;
- A clarification of the geographical scope of the regime to avoid regulatory arbitrage;
- An a posteriori check over AML-CFT arrangements that actors must implement, rather than an a priori control that is stricter that the FATF recommendations and impose long delays before launching a new activity;
- More efficient enforcement mechanisms for credit institutions to provide banking services (accounts, loans, etc.) for actors that comply with the rules of the regime.

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

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

5000 character(s) maximum

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

Building a bespoke regime for crypto-assets and crypto-asset service providers should lean on the following principles:

- Flexibility and scalability. As stated above, the traditional categorization of crypto-assets (payment, investment, utility and hybrid tokens) should be dropped. A better approach seems to distinguish crypto-assets that legally qualify under current regulations from others. Within “others”, “cryptocurrencies” and “tokens/(programmable) crypto-assets” should be subject to adjustable requirements depending on the activity/service provided, the intrinsic features of assets and their risk profile.

- Proportionality. For crypto-assets that legally qualify under current regulations from others, legal adjustments should be considered in the light of the inadequacy of some rules to crypto-asset markets and the benefits that the blockchain technology brings in terms of safety, liquidity, cyber-resilience, etc. For others, some key facts should be kept in mind when designing their regulation. For example, crypto-crypto activities raise less risks in terms of AML-CFT than crypto-fiat ones. Also, the provision of tokens to clients in order to make them access to their services should not be a regulated activity.

- Efficiency. Regulatory frameworks for crypto-assets should not only focus on the features of crypto-assets, but also on activities/services and the specific risks arising from the combination of the assets' features and the activities/services provided on these assets.

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

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

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

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

N/A

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

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

More generally, legal certainty in any aspect of regulation is a positive catalyst for an economic sector. If ADAN did not deeply investigate the prudential treatment of financial institutions' exposures to crypto-assets at this time, our preliminary analysis is that clarity in this area could reassure banks and prompt them to better explore the opportunities of decentralized finance, not only as spectators or commercial partners but also as potential players.

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

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

In general, harmonisation of laws within the European Union is a favorable evolution for any business. If at this stage, ADAN did not deeply investigate this topic lacking the required expertise, our preliminary

conclusion is that convergence in national civil laws could facilitate inherently cross-border activities on crypto-assets within the European Union, and even galvanize intra-EU synergies.

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

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

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

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

The French regime for crypto-assets set rules for both token issuers and digital asset service providers (PSAN). See answer to question 15.
Article L.552-3 of the French Monetary and Financial Code defines the issuance of crypto-assets as “an offer of tokens to the public [that] consists of offering the public, in whatever form, to subscribe to these tokens. The offer of tokens open to subscription to a limited number of persons [150 people] acting on their own account does not constitute an offer of tokens to the public.”

Article L. 552-2 of the French Monetary and Financial Code defines a “token” as “any intangible asset representing, in digital form, one or more rights that can be issued, registered, stored or transferred by means of a shared electronic recording device making it possible to identify, directly or indirectly, the owner of said asset”

Article L. 54-10-2 of the French Monetary and Financial Code defines “digital asset services” as:
1° Custody of digital assets ;
2° Buying or selling digital assets against legal money (“crypto-fiat exchange”) ;
3° Exchange of digital assets with other digital assets (“crypto-crypto exchange”) ;
4° Operation of a digital asset trading venue ;
5° Other services on digital assets such as:
- RTO on behalf of clients ;
- Portfolio management ;
- Investment advice ;
- Underwriting on a firm commitment basis ;
- Placing on a firm commitment basis ;
- Placing without a firm commitment basis.

1. Issuance of crypto-assets

This section distinguishes between the issuers of crypto-assets in general (1.1.) and the issuer of the so-called "stablecoins" backed by a reserve of real assets (1.2.).

1.1. Issuance of crypto-assets in general

The crypto-asset issuer or sponsor is the organisation that has typically developed the technical specifications of a crypto-asset and set its features. In some cases, their identity is known, while in some cases, those promoters are unidentified. Some remain involved in maintaining and improving the crypto-asset's code and underlying algorithm while other do not (study from the European Parliament on "Cryptocurrencies and Blockchain", July 2018). Furthermore, the issuance of crypto-assets is generally accompanied with a document describing crypto-asset and the ecosystem around it, the so-called 'white papers'. Those 'white papers' are, however, not standardised and the quality, the transparency and disclosure of risks vary greatly. It is therefore uncertain whether investors or consumers who buy crypto-assets understand the nature of the crypto-assets, the rights associated with them and the risks they present.

Question 20. Do you consider that the issuer or sponsor of crypto-assets marketed to EU investors/consumers should be established or have a physical presence in the EU?

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

20.1 Please explain your reasoning for your answer to question 20:

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

Not necessarily.

Token issuances are offered to the public via the Internet. Intrinsically, the Internet has no "geographical" boundaries. That is why it seems hard to supervise that EU citizens only subscribe to EU token offerings (what they do not always know or care). To the same extent, preventing EU consumers from using a crypto-asset service that is available on the Internet is practically very complicated.

Rather than setting a geographical condition, a more efficient approach would be that token issuers - as well as service providers - from third countries get an authorization, based on the same set of conditions than those established in the EU, to be able to offer their services to EU citizens. This is also likely to foster competition within the industry and increase the quality of issuance and services provided. When they comply with such requirements, they would be "white listed" so people could check it before subscribing to a token offering or invoking crypto-asset services.

The problem arising from the lack of geographical boundaries is the difficulty to establish a passport mechanism like Prospectus'. On the one hand, if an issuer does not establish himself in an identified country, the home State authority that is competent to deliver the authorization cannot be identified. On the other hand, if an issuer does not identify all countries where investors subscribed to his issuance, the home State cannot ensure host States that the white paper complies with regulatory requirements.

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

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

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

5000 character(s) maximum

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

Proper information about a token issuance is essential to enable interested parties to take their investment decisions with a sound knowledge of the project that they fund, the terms of the offering, and the risks that they run.

The issuer is the best to disclose the right information about his tokens. In case he uses the service of other entities that make the connection with potential purchasers, they should act as information relays with them.

The "white paper" should contain minimum information about:

- The issuer: a presentation of the person issuing the tokens (legal identity, past experience, areas of expertise, etc...) and the project;
- The main features of the token offer: subscription period, fundraising goal (amount/range), prospective use of funds, legal money or cryptocurrency or stablecoins accepted, applicable law and competent jurisdiction;
- Tokens issued: utility, rights associated with tokens, subscription price, admissibility for trading on crypto exchanges (if so);
- The blockchain technology: "yellow paper", technical architecture, smart contracts;
- Arrangements implemented in terms of:
- Safeguarding and redeemability of assets collected;
- AML-CFT;
- The main risk factors in terms of:
- Liquidity: change, pricing, lack of secondary trading (where appropriate);
- Cyber-security: errors and security breaches (hacking, data theft), loss or theft of private key media (when there is one, which are not concerned the case), linked to the monitoring and safeguarding of assets, linked to blockchain and exchange platforms;
- The evolution of the project: failure (launch or development technical and operational aspects of the project), substantial modification of the project and the rights added to the tokens, absence of regular communication from the part of the issuer on its project or on any event that may have an impact on the project;
- Legal risks (for non-EU potential subscribers).

Question 22. If a requirement to provide the information on the offers of crypto-assets is imposed on their issuer/sponsor, would you see a need to clarify the interaction with existing pieces of legislation that lay down information requirements (to the extent that those rules apply to the offers of certain crypto-assets, such as utility and/or payment tokens)?

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

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

22.1 Is there any other existing piece of legislation laying down information requirements with which the interaction would need to be clarified? Please specify which one(s) and explain your reasoning:

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

N/A

22.2 Please explain your reasoning and indicate the type of clarification (legislative/non legislative) that would be required:

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

More generally, limitation of legal risks in any aspect of regulation is crucial to provide with the necessary visibility for economic actors. If ADAN did not deeply investigate these pieces of regulation, it is likely that the industry will raise such questions at one time and expect answers from competent authorities.

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

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

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
The managers of the issuer or sponsor should be subject to fitness and probity standards	○	○	◉	○	○	○
The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions	○	○	○	◉	○	○
Where necessary, the issuer or sponsor should put in place a mechanism to safeguard the funds collected such as an escrow account or trust account	○	○	○	◉	○	○

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

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

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

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

Even after the token sale, the issuer should be able to communicate continuous information about the progress of the fundraising, the allocation of tokens to subscribers, the use of funds, the main evolutions of the project, etc.

Under the new French legal framework, the fulfillment of their obligations grants token issuers that got the AMF's visa with some important guarantees:

- First, token issuers cannot be refused access by credit institutions to deposit and payment account services . For such a refusal, or if they did not answer to the actor's request by 2 months, credit institutions must provide the French authorities (the AMF and the ACPR) with the reasons for this refusal. The ACPR can then offer actors the possibility to ask the French Central Bank for appointing one credit institution to provide required services.
- Second, their tokens become eligible assets for some investment vehicles (up to a 20% threshold).

1.2. Issuance of "stablecoins" backed by real assets

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

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

5000 character(s) maximum

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

Although we consider that the distinction between stablecoin and global stablecoin is artificial at best, the objective criteria of distinction would probably be the availability of the stablecoin outside of the reference asset area. e.g. a stablecoin against the euro that would be widely available outside of the eurozone would be considered a global stablecoin.

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

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

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

Question 25.1 To tackle the specific risks created by "stablecoins" and "global stablecoins", what are the requirements that could be imposed on

their issuers and/or the manager of the reserve?

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

	Relevant	Not relevant	Don't know / no opinion
The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)	◉	○	○
The issuer should contain the creation of "stablecoins" so that it is always lower or equal to the value of the funds of the reserve	◉	○	○
The assets or funds of the reserve should be segregated from the issuer's balance sheet	◉	○	○
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	◉	○	○
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	◉	○	○
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	◉	○	○
Obligation for the assets or funds to be held in custody with credit institutions in the EU	○	◉	○
Obligation for the assets or funds to be held for safekeeping at the central bank	◉	○	○
Periodic independent auditing of the assets or funds held in the reserve	◉	○	○
The issuer should disclose information to the users on (i) how it intends to provide stability to the "stablecoins", (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve	◉	○	○
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	◉	○	○
Obligation for the issuer to use open source standards to promote competition	◉	○	○

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

5000 character(s) maximum

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

N/A

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

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

For the moment, an obligation for the assets or funds to be held in custody with credit institutions in the EU is not pragmatic considering the reluctance of such institutions to investigate crypto-asset activities. In France for instance, actors encounter serious difficulties when they try to establish a business relation with the French banking sector. That is why this obligation would only put the brakes on the development of stablecoin projects.

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

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

	Relevant	Not relevant	Don't know / no opinion
The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...)	◉	○	○
The issuer should contain the creation of "stablecoins" so that it is always lower or equal to the value of the funds of the reserve	◉	○	○
The assets or funds of the reserve should be segregated from the issuer's balance sheet	◉	○	○
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	◉	○	○
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	◉	○	○

The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	◉	○	○
Obligation for the assets or funds to be held in custody with credit institutions in the EU	○	◉	○
Periodic independent auditing of the assets or funds held in the reserve	◉	○	○
The issuer should disclose information to the users on (i) how it intends to provide stability to the "stablecoins", (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve	◉	○	○
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	◉	○	○

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

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

N/A

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

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

For the moment, an obligation for the assets or funds to be held in custody with credit institutions in the EU is not pragmatic considering the reluctance of such institutions to investigate crypto-asset activities. In France for instance, actors encounter serious difficulties when they try to establish a business relation with the French banking sector. That is why this obligation would only put the brakes on the development of stablecoin projects.

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

Question 26. Do you consider that wholesale "stablecoins" (those limited to financial institutions or selected clients of financial institutions, as opposed

to retail investors or consumers) should receive a different regulatory treatment than retail "stablecoins"?

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

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

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

We consider "wholesale stablecoins" to be a new settlement layer between the financial institutions. The regulatory treatment should be adapted to this very specific use case, that widely differs from the commonly accepted notion of "stablecoin".

2. Trading platforms

Trading platforms function as a market place bringing together different crypto-asset users that are either looking to buy or sell crypto-assets. Trading platforms match buyers and sellers directly or through an intermediary. The business model, the range of services offered and the level of sophistication vary across platforms. Some platforms, so-called 'centralised platforms', hold crypto-assets on behalf of their clients while others, so-called decentralised platforms, do not. Another important distinction between centralised and decentralised platforms is that trade settlement typically occurs on the books of the platform (off-chain) in the case of centralised platforms, while it occurs on DLT for decentralised platforms (on-chain). Some platforms have already adopted good practice from traditional securities trading venues[19] while others use simple and inexpensive technology.

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

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

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

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

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

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

5000 character(s) maximum

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

N/A

27.2 Please explain your reasoning for your answer to question 27:

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

Most of the risks mentioned can be managed by trading venues without specific difficulties attributable to their activity.

One risk gives more cause for concerns: losses of users' crypto-assets through theft or hacking (cyber risks). A recent study of The Block Genesis indicates that cryptocurrency exchange hacks surpass $1.3 billion all time (https://www.theblockcrypto.com/genesis/17876/research-cryptocurrency-exchange-hacks-surpass-1-3-billion-all-time-61-coming-from-2018).

It has to be noted that this risk is higher when users manage to store their assets with their own resources (self-custody).

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

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

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
Trading platforms should have a physical presence in the EU	○	○	◉	○	○	○
Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)	○	◉	○	○	○	○
Trading platforms should segregate the assets of users from those held on own account	○	○	○	◉	○	○
Trading platforms should be subject to rules on conflicts of interest	○	○	◉	○	○	○

Trading platforms should be required to keep appropriate records of users' transactions	○	○	◉	○	○	○
Trading platforms should have an adequate complaints handling and redress procedures	○	○	○	◉	○	○
Trading platforms should be subject to prudential requirements (including capital requirements)	○	◉	○	○	○	○
Trading platforms should have adequate rules to ensure fair and orderly trading	○	○	◉	○	○	○
Trading platforms should provide access to its services in an undiscriminating way	○	○	◉	○	○	○
Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse	○	○	◉	○	○	○
Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)	○	◉	○	○	○	○
Trading platforms should be responsible for screening crypto-assets against the risk of fraud	○	○	◉	○	○	○

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

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

N/A

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

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

Most of the rules should apply to crypto-assets in general. However, some specific features could lead to some finetuning in terms of assets allowed to be listed, listing/delisting procedures, etc..

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

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

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

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

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

assets against fiat currency (conversion risk)	◉	○	○	○	○	○
Absence of transparent information on the crypto-assets proposed for exchange	○	◉	○	○	○	○

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

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

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

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

Most of the risks mentioned can be managed by exchanges. The difficulties identified are not specifically attributable to their activity.

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

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

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

Exchanges should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)	○	◉	○	○	○	○
Exchanges should segregate the assets of users from those held on own account	○	○	◉	○	○	○
Exchanges should be subject to rules on conflicts of interest	○	◉	○	○	○	○
Exchanges should be required to keep appropriate records of users' transactions	○	○	◉	○	○	○
Exchanges should have an adequate complaints handling and redress procedures	○	○	◉	○	○	○
Exchanges should be subject to prudential requirements (including capital requirements)	○	○	○	◉	○	○
Exchanges should be subject to advertising rules to avoid misleading marketing/promotions	○	○	○	◉	○	○
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)	○	○	◉	○	○	○
Exchanges should be responsible for screening crypto-assets against the risk of fraud	○	◉	○	○	○	○

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

5000 character(s) maximum

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

N/A

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

5000 character(s) maximum

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

No.

4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys[20] and to interact with DLT to allow users to send and receive crypto-assets and monitor their balances. Crypto-asset wallets come in different forms. Some support multiple crypto-assets/DLTs while others are crypto-asset/DLT specific[21]. DLT networks generally provide their own wallet functions (e.g. Bitcoin or Ether).

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

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

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

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

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

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant
No physical presence in the EU	◉	○	○	○	○	○
Lack of adequate governance arrangements, including operational resilience and ICT security	○	○	○	◉	○	○
Absence or inadequate segregation of assets held on the behalf of clients	○	○	◉	○	○	○
Conflicts of interest arising from other activities (trading, exchange)	◉	○	○	○	○	○

Absence/inadequate recordkeeping of holdings and transactions made on behalf of users	○	◉	○	○	○	○
Absence/inadequate complaints or redress procedures are in place	○	○	◉	○	○	○
Bankruptcy of the custodial wallet provider	○	○	◉	○	○	○
Inadequate own funds to repay the consumers	◉	○	○	○	○	○
Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)	○	○	○	○	◉	○
The custodial wallet is compromised or fails to provide expected functionality	○	○	○	◉	○	○
The custodial wallet provider behaves negligently or fraudulently	○	○	◉	○	○	○
No contractual binding terms and provisions with the user who holds the wallet	○	◉	○	○	○	○

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

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

N/A

31.2 Please explain your reasoning for your answer to question 31:

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

Most of the risks mentioned can be managed by custodians. The difficulties identified are not specifically attributable to their activity.

Provided that the custodial wallet providers always keep the amount of crypto-assets they have in custody and do not function with fractional reserves (as the market practice is today), we believe that the main risks related to custodial wallets are related to losing the access to the funds, either because they are stolen or because the custodian loses access to the funds for any other reason:

- Security: The custodian can lose access to the funds of the customer due to a hack, theft, etc...
- Technical: The custodian can lose access to the funds due to a technical mistake, shutdown, hardware or software malfunction, physical loss of any document where the private keys can be stored, etc…

- Governance: if the governance is badly defined or controlled, the control of the funds can be lost by the relevant party.

We believe that any regulation of the custodial wallet providers should cover those points. It has to be noted that some of those risks can be mitigated by subcontracting part of the functions essential to proper custody services to technical experts. In this case, the quality of the technical solution may be assessed by the national authorities.

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

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

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

Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions	◉	○	○	○	○	○
Custodial wallet providers should be subject to certain minimum conditions for their contractual relationship with the consumers/investors	○	○	○	◉	○	○

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

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

A technical / security audit of the custodian wallet provider or the subcontracting of those functions to an audited / certified services provider may be imposed on custodians wallet providers.

Those risks could also be mitigated by insurance or minimum capital requirements.

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

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

No. Optimum security should be a mix of technological security (use of hardware and software that have shown their resilience to hacks) and secure processes (strong governance within the custodian to prevent theft through collusion for example).

That is why it seems important for the development of an European industry of custodians that regulations applying to them be the most consistent possible whatever the type of crypto-assets is. First, one client is likely to hold different legal types of crypto-assets on one single private key. Therefore this could be very detrimental to European actors wishing to design an attractive offer if complying with too divergent rules according to different crypto-assets appears very burdensome. Second, custody of crypto-assets whatever they are legally qualified requires the same technical expertise and arrangements. It would make few sense that requirements in terms of security, safeguarding, reporting, etc. be different.

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

- ◉ Yes
- ○

No

Don’t know / no opinion / not relevant

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

5000 character(s) maximum

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

As we advocate that crypto-assets that comply with the MiFID II “financial instrument” definition must fall within the same regulatory package, this implies that custodian that provides “safekeeping and administration of financial instruments for the account of clients, including custodianship and related services such as cash/collateral management and excluding maintaining securities accounts at the top tier level” must be authorised by the national competent authority.

However, according to our guiding principle (see part II), a review of the obligations applying to them should be conducted to better fit the specific features (especially technical) of crypto-assets and rationalise the current regulatory framework considering the guarantees that blockchain provides in terms of security, cyber-resilience, transparency, etc. Simplification of some current rules could go with creation of new ones that better assess the risk arising from the custody of crypto-assets and that could not be taken into account before their emergence.

To that end, an analysis of the following provisions should determine if they are relevant in the crypto-asset universe and how they could be adapted. Such work could be accomplished by the EU digital lab proposed by the AMF.

This is likely, and desirable (see answer to question 33) that such legal adjustments for “security tokens” converge towards the appropriate regulatory framework that should apply to custodians of “tokens” and “crypto-assets”.

Article 16 of MiFID 2, paragraphs 8 and 9, requires that actors that hold financial instruments and funds belonging to clients must “make adequate arrangement” to safeguard the rights of clients and prevent the use of their assets for their own account.

Article 59 of Delegated Regulation 2017-565 of 25 April 2016 displays the information concerning safeguarding of client financial instruments or client funds that must be communicated to clients:

- if their assets are held by a third party on behalf of the custodian,
- if their assets are held an omnibus account by a third party,
- if their assets cannot be separately identifiable from the proprietary financial instruments of that third party,
- if accounts that contain their assets are or will be subject to the law of a jurisdiction other than that of a Member State,
- the existence and the terms of any security interest or lien which the custodian has or may have over the client's assets, or any right of set-off it holds in relation to those assets,
- if the custodian is entering into securities financing transactions in relation to financial instruments held by it on behalf of a client, or using such financial instruments for its own account or the account of another client with clear, full and accurate information on the obligations and responsibilities of the custodian

Articles 2 to 8 of Delegated Directive 2017-593 of 7 April 2016 set various requirements for actors that provide for the safeguarding of financial instruments. These provisions focus on reporting and record-keeping, information reconciliation, segregation of assets, risk mitigation, depositing of clients’ assets and the adequate use of these assets.

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

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

No. Other business models of activities and services in relation to digital wallets should be kept outside of the regulatory field.

5. Other services providers

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

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

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

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

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion / not relevant

Reception and transmission of orders in relation to crypto-assets	◉	○	○	○	○	○
Execution of orders on crypto-assets on behalf of clients	◉	○	○	○	○	○
Crypto-assets portfolio management	○	○	◉	○	○	○
Advice on the acquisition of crypto-assets	○	○	◉	○	○	○
Underwriting of crypto-assets on a firm commitment basis	○	○	◉	○	○	○
Placing crypto-assets on a firm commitment basis	○	○	◉	○	○	○
Placing crypto-assets without a firm commitment basis	○	○	◉	○	○	○
Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)	◉	○	○	○	○	○
Processing services, also known as 'mining' or 'validating' services in a DLT environment (e.g. 'miners' or validating 'nodes' constantly work on verifying and confirming transactions)	◉	○	○	○	○	○
Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)	○	○	◉	○	○	○
Services provided by developers that are responsible for maintaining/updating the underlying protocol	◉	○	○	○	○	○
Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)	○	○	◉	○	○	○

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

5000 character(s) maximum

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

N/A

35.2 Please illustrate your response to question 35 by underlining the potential risks raised by these services if they were left unregulated and by identifying potential requirements for those service providers:

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

The main risks where the actors identified as relevant are not regulated at all would be market integrity and conflicts of interest.

The two services “reception and transmission of orders in relation to crypto-assets” and “execution of orders on crypto-assets on behalf of clients” do not illustrate the current functioning of crypto-assets markets. There is currently no use of such services and defining a regulatory framework for these providers should not be a priority.

To the extent that information services for financial markets (such as Bloomberg and Thomson Reuters) are not regulated, information services for crypto-assets should not fall under the regulatory regime applying to crypto-asset service providers.

Both processing services and blockchain protocol maintaining/updating services should not be considered as regulated crypto-asset services as they are responsible for the smooth technical functioning of blockchain networks for the common interest of participants, and do not pose any risk to them.

With respect to the agents of issuers, if we understand correctly, this question is related to the development of issuance of crypto-assets through an intermediary that manages the issuance and the sale of the crypto-asset on behalf of the issuer. Our opinion is that this means of issuance will likely develop in the future; and that any regulation put in place should encompass this reality and allow those actors to be regulated and for the passing-through of regulatory expectations from the intermediary to the issue - where if the intermediary is regulated and already applies KYC/AML regulation, the issuer’s obligations should be limited to some extent.

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

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

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

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

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

No, in general. This is especially the case since we consider that none of the payments made using crypto-assets are using services “making payment transactions”.
Payments by crypto-assets are usually done using two distinct means:
- A professional directly accepts crypto-assets as a means of payment. In this case, the client sends the crypto-assets to the seller’s account on the blockchain. The seller keeps the assets or later sells them against other assets or fiat currency.
- A professional is using a service to accept crypto-assets, that will take the payment on his behalf, convert the crypto-asset to fiat currency, and give them the proceeds of the sale minus a commission.

In both cases, the client is sending the crypto-assets directly - he is not using a centralized party whose activity is making payment transactions. This is still true under the assumption of using a layer 2 payment channel like Lightning Network, provided that the payment channel is sufficiently decentralized and no central operator can be identified.

It is our opinion that the operators of a decentralized layer 2 payment channel solution should not be regulated as their only function is to apply the rules of the layer 2 protocol against the payment of a fee, eventually.

Where the payment channel is sufficiently decentralized, the function rendered is very similar to the operations made by a miner in a public blockchain - and therefore should not be considered as a “making payment transaction” under the rules of PSD2.

C. Horizontal questions

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

1. Market Integrity

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

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

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

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don’t know / no opinion /

						not relevant
Price manipulation	○	○	◉	○	○	○
Volume manipulation (wash trades…)	○	◉	○	○	○	○
Pump and dump schemes	○	◉	○	○	○	○
Manipulation on basis of quoting and cancellations	○	◉	○	○	○	○
Dissemination of misleading information by the crypto-asset issuer or any other market participants	○	○	◉	○	○	○
Insider dealings	○	○	○	○	◉	○

37.1 Is there any other big market integrity risk related to the trading of crypto-assets not mentioned above that you would foresee? Please specify which one(s) and explain your reasoning:

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

N/A

37.2 Please explain your reasoning for your answer to question 37:

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

Volume manipulation, pump and dump schemes and manipulation on the basis of quoting and cancellations are existing risks that prevails on the most illiquid crypto-assets, although it should be noted that it would mostly impact bigger trades. In addition, on liquid assets (such as bitcoins and ethers), such market abuses are very difficult to implement without being detected.

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

Question 38. In your view, how should market integrity on crypto-asset markets be ensured?

5000 character(s) maximum

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

The market integrity of crypto-asset exchanges is a very complex subject due to:

- the multinational nature of those crypto-assets that allows for trading in any jurisdiction, and
- the existence of decentralized or semi-decentralized services that operate without limitations and without prior identification of clients.

The EU could, and should probably, ensure that market integrity is respected through the crypto to fiat trades, by implementing rules that would allow proper supervision of those trades and reporting of any insider trading, price manipulation, volume manipulation… This should be complemented by a set of sanctions.

In order to ensure the proper supervision of the market integrity of crypto-assets in the long run, we believe that two components are essential:

- the creation or designation of a dedicated regulatory body - a crypto-asset markets regulator, both at the EU level and in each of the EU countries.
- the development of a set of tools at EU or state levels to identify patterns of transactions or bad actors and develop the regulatory and legal framework to ban them from operating with EU clients.

While the information on executed transactions and/or current balance of wallets are often openly accessible in distributed ledger based crypto-assets, there is currently no binding requirement at EU level that would allow EU supervisors to directly identify the transacting counterparties (i.e. the identity of the legal or natural person(s) who engaged in the transaction).

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

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

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

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

This would depend on the way the transaction is conducted. In some cases, identifying the parties would make sense. As an example, if the issuer of crypto-assets sells all its assets to the market without notice to the general public, this could be considered as an insider trade.

For centralized exchanges, it would be possible for the supervisors to identify the parties to a transaction and some controls may be put in place for some individuals and some crypto-assets. However, it has to be noted that:

- The crypto-assets can be sold and bought anywhere in the world. Most assets are listed either outside of the EU or both inside or outside of the EU. There’s no easy path for a cross-border regulation that would allow EU supervisors to ask foreign exchanges for that information, especially where those exchanges do not ask for any identification of clients (this practice is still common for exchanges between crypto-assets).
- More and more exchanges between crypto-assets are done through decentralized exchanges. Those

exchanges are operated directly on the blockchain and provide two distinct sets of features: they are accessible from anywhere and to anyone, and all the trades are executed publicly on the blockchain and are auditable by a third party.

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

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

There's no proper way of being 100 % ensured that any requirement that the EU would put in place are not circumvented by trading on platforms/exchanges in third countries, except in the case where an international regulatory body is implemented with the powers to sanction any platform/exchange that would not respect international requirements.

2. Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT)

Under the current EU anti-money laundering and countering the financing of terrorism (AML/CFT) legal framework (Anti-Money Laundering Directive (Directive 2015/849/EU) as amended by AMLD5 (Directive 2018/843/EU)), providers of services (wallet providers and crypto-to-fiat exchanges) related to "virtual currency" are "obliged entities". A virtual currency is defined as: "*a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically". The Financial Action Task Force (FATF) uses a broader term "virtual asset" and defines it as: "a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations*". Therefore, there may be a need to align the definition used in the EU AML/CFT framework with the FATF recommendation or with a "crypto-asset" definition, especially if a crypto-asset framework was needed.

Question 41. Do you consider it appropriate to extend the existing "virtual currency" definition in the EU AML/CFT legal framework in order to align it with a broader definition (as the one provided by the FATF or as the definition of "crypto-assets" that could be used in a potential bespoke regulation on crypto-assets)?

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

41.1 Please explain your reasoning for your answer to question 41:

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

The definition of virtual assets provided by the FATF is a good starting point. This definition could be specified to exclude specifically all the “digital goods” (e.g. cryptokitties, ENS or similar domain names, etc.) or tokens that represent a right to a preexisting good or service (e.g.: a ticket for the theatre, a pair of socks…).

This being said, the position of ADAN on AML-KYC procedures applied to crypto-assets is the following: There’s an obvious need for AML-KYC procedures in the crypto-assets markets, and we are pushing for the extension of good practices in the field. We believe that crypto-assets specificities command for adapted practices. The characteristics of those assets are a unique opportunity to modernize the existing procedures and allow for more AML automatization and use of Deep Learning capabilities on the chain. This would allow for a more timely and efficient flagging of suspect transactions, and reduce frictions to entry for all the participants. Therefore, it does not make sense to simply extend the existing obligations to the crypto-assets - rather, a new set of obligations should be determined at the EU or local level with a regulatory body that would be fully adapted to the world of crypto-assets (either an entirely new section inside existing regulatory bodies or a dedicated one).

In order to determine the best way to implement AML procedures tailored to the crypto-assets sector, we recommend the creation of a dedicated task force that would include representatives of all the industry, including so-called “VASPs”, other actors of the industry (non-VASPs using crypto-assets in the course of their activities) and professional associations. It has to be noted that although AML service providers should be heard during those working groups, they should not be allowed to conclude on any necessary measure (due to obvious potential conflict of interests).

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

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

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

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

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

Most of the AML-KYC risks are located at the gateways (i.e. crypto-to-fiat conversions). It should be emphasized that the regulation of those gateways should be mandatory in all of the EU, with an unified regime and passporting.

At the moment, we don't see any urgency to extend the scope of the mandatory AML-CFT framework. Crypto-to-crypto venues can in some edge cases facilitate money laudering or financing of terrorism when no AML-KYC measures are in place at the level of the company, but this potential increase of the risk is entirely mitigated at the gateway level, as the crypto-to-fiat venue will apply required AML-CFT measures at the time of cashout.

Question 43. If a bespoke framework on crypto-assets is needed, do you consider that all crypto-asset service providers covered by this potential framework should become 'obliged entities' under the EU AML/CFT framework?

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

43.1 Please explain your reasoning for your answer to question 43:

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

No. See answer above.

Question 44. In your view, how should the AML/CFT risks arising from peer-to-peer transactions (i.e. transactions without intermediation of a service provider) be mitigated?

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

The proper way of mitigating the AML-CFT risk arising from those transactions is to operate at the gateway level (crypto-to-fiat transactions).

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

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

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

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

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

General guidance and principles should be determined that would help local authorities implement practically those adapted AML-KYC procedures.

It is important to adapt such guidelines to the specificities of the crypto-industry, that are: it is a nascent ecosystem composed of start-ups and small and medium enterprises, whose volume of activities (including trading volume on crypto-assets) are far from orders of magnitude prevailing in traditional financial markets. Moreover, as there is a large number of very new actors, guidelines could be more pedagogic: compared with long-established entities, they are less likely to have legal and compliance experts being able to perfectly decrypt the regulatory framework applying to them. The AMF has already acknowledged this reality and published their synthesis on "AMF-CFT: Summary of the main measures to be implemented by service providers on digital assets": https://www.amf-france.org/sites/default/files/2020-02/lcb-ft-.pdf

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

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

	1 (completely irrelevant)	2	3	4	5 (highly relevant)	Don't know / no opinion /

						not relevant
Directors and senior management of such providers should be subject to fit and proper test from a money laundering point of view, meaning that they should not have any convictions or suspicions on money laundering and related offences	○	○	○	◉	○	○
Service providers must be able to demonstrate their ability to have all the controls in place in order to be able to comply with their obligations under the anti-money laundering framework	○	○	○	◉	○	○

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

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

Those two requirements are good practice and help ensure that the AML/KYC procedures are properly managed.

However, it has to be noted that those requirements should be adapted as follows:
- the AML/CFT training should be, as much as possible, adapted to the crypto-asset industry specifically;
- the cost of compliance to those two requirements should be low (in order to avoid the creation of significant barriers to entry to this nascent market). In this regard, the creation of reference documents and training delivered by the regulator or a professional organization for a low price would help.

3. Consumer/investor protection[21]

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

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

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

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

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

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

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

5000 character(s) maximum

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

N/A

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

5000 character(s) maximum

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

The requirements should apply to all crypto-assets (but not to digical goods or other representations of goods or services on blockchain).

All of the proposed requirements make sense, to the notable exception of general investment limits. In addition to being extremely difficult to put in place (due to the very large number of service providers in the space), this would be an unjustified restriction to the individual's freedom. As long as the individuals are correctly informed of the risks taken, they should be able to manage their assets at will. This is especially true since such restrictions do not exist with other investment vehicles.

Of course, this position is not exclusive from specific investment limits that actors should put in place depending on the profile of their clients (appropriateness and sustainability tests).

Question 48. Should different standards of consumer/investor protection be applied to the various categories of crypto-assets depending on their prevalent economic (i.e. payment tokens, stablecoins, utility tokens, ...) or social function?

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

48.1 Please explain your reasoning for your answer to question 48:

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

We don't see any significant reason to apply different levels of consumer/investor protection. The information provided on the asset should of course be adapted to the nature of the asset and the risks borne, but there's no significant reason to adapt the scope or the weight of those obligations (provided that we are excluding value representations that are not falling into the scope of "crypto-assets").

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

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

- Yes
- No

- Don’t know / no opinion / not relevant

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

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

No, information provided should be identical.

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

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

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

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

Airdrops are very specific and usually done to get the attention of an investor on a product. As they are allocated for free, it’s possible that some of the requirements should be alleviated (e.g. the risks of losing capital invested, not relevant in this case).

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

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

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

	1				5	Don’t know /

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

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

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

N/A

51.2 Please explain your reasoning for your answer to question 51:

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

This question raised a lot of interrogations with our members. We concluded that there's no reason to ban or limit the access to any kind of asset to the EU consumers/investors:

- It's difficult and sometimes impossible to determine the country of issuance of a crypto-asset. As an example, the cryptocurrencies have no identified issuer and no identified country of origin. Some assets are issued by DAOs or decentralized projects that are not registered in any country.
- It would be very difficult to control those operations from the EU.
- It would be much more efficient to control the listing of those assets for secondary markets on EU-based or EU-regulated exchanges.

4. Supervision and oversight of crypto-assets service providers

As a preliminary remark, it should be noted that where a crypto-asset arrangement, including "stablecoin" arrangements qualify as payment systems and/or scheme, the Eurosystem oversight frameworks may apply. In accordance with its mandate, the Eurosystem is looking to apply its oversight framework to innovative projects. As the payment landscape continues to evolve, the Eurosystem oversight frameworks for payments instruments, schemes and arrangements are currently reviewed with a view to closing any gaps that innovative solutions might create by applying a holistic, agile

and functional approach. The European Central Bank and Eurosystem will do so in cooperation with other relevant European authorities. Furthermore, the Eurosystem supports the creation of cooperative oversight frameworks whenever a payment arrangement is relevant to multiple jurisdictions.

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

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

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

Direct supervision by the European Authorities would not be efficient nor cost-effective. We recommend supervision at a national level with coordination at the EU level, in order to ensure a certain level of harmonization between practices.

From a practical perspective, we would recommend an ad hoc regulatory body, possibly in relation with a self-regulatory body that could help keep processes and create a first level regulation delegated by member States.

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

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

Our opinion is that this question is a bit premature. We recommend a period where the answers to this consultation are analyzed and 1-to-1 exchanges are opened with the national regulators, industry players and associations. From there, good practices can be inferred and adapted tools chosen or developed at the EU or national level.

As a professional association, we are dedicated to ensuring good practices from the industry players and are already working on guidelines for both the regulators and the players.

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

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

A. General questions on 'security tokens'

Introduction

For the purpose of this section, we use the term 'security tokens' to refer to crypto-assets issued on a DLT and that qualify as transferable securities or other types of MiFID financial instruments. By extension, activities concerning security tokens would qualify as MiFID investment services/activities and transactions in security tokens admitted to trading or traded on a trading venue[23] would be captured by MiFID provisions. Consequently, firms providing services concerning security tokens should ensure they have the relevant MiFID authorisations and that they follow the relevant rules and requirements. MiFID is a cornerstone of the EU regulatory framework as financial instruments covered by MiFID are also subject to other financial legislation such as CSDR or EMIR, which therefore equally apply to post-trade activities related to security tokens.

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

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

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

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

Current trends concerning security tokens

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

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

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

The Commission services' understanding is that permissionless networks and decentralised platforms[29]are still in their infancy, with uncertain prospects for future applications in financial services due to their higher trade latency and lower liquidity. Permissionless decentralised platforms could potentially develop only at a longer time horizon when further maturing of the technology would provide solutions for a more efficient trading architecture. Therefore, it could be premature at this point in time to make any structural changes to the EU regulatory framework.

Security tokens are, in principle, covered by the EU legal framework on asset management in so far as such security tokens fall within the scope of "financial instrument" under MiFID II. To date, however, the examples of the regulatory use cases of DLT in the asset management domain have been incidental.

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

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

---

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

[26] See section IV.2.5 for further information

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

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

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

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

5000 character(s) maximum

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

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

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

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

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

Tokenization can bring great benefits in the current functioning of financial markets and market infrastructures:

- For those which are not already digitalised (in France, all securities have had to be dematerialised since 1981), tokenisation can prompt generalization of paperless financial instruments then automation of many processes. This constitutes a good starting point to reduce operating errors due to manual processing, then the global costs of human errors, and to increase efficiency.
- Automation. The smooth functioning of financial markets is based on many record-keeping held by various parties. Automation through smart contracts would help manage them and guarantee continuous and right reconciliations among them.
- Transparency and trustworthiness. Smart contracts enable the automatic execution of operations when (and only when) all conditions are met, as they were initially encoded in the smart contract. All authorized parties can access the ledger to check which operations have been executed, and smart contracts to verify how they were programmed. This is a substantial confidence enhancer for all interested parties, from counterparties to transactions, business partners to regulators if they wish to use blockchain in their supervision missions.
- Liquidity. Tokenisation can boost - or even create - liquidity for some intrinsically illiquid assets. This can cover shares that are not traded on secondary markets, venture capital and real estate industries.
- Cyber-resilience. Distributed ledgers are the “single version of the truth” kept in a decentralized way so

no central point of failure can be identified in the context of cyber-attacks. This is a very substantial benefit for crucial activities that financial ones are, even more when they pose a systemic risk to financial stability.

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

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

Tokenization can bring great benefits in the current functioning of financial markets and market infrastructures:

- For those which are not already digitalised (in France, all securities have had to be dematerialised since 1981), tokenisation can prompt generalization of paperless financial instruments then automation of many processes. This constitutes a good starting point to reduce operating errors due to manual processing, then the global costs of human errors, and to increase efficiency.
- Automation. The smooth functioning of financial markets is based on many record-keeping held by various parties. Automation through smart contracts would help manage them and guarantee continuous and right reconciliations among them.
- Transparency and trustworthiness. Smart contracts enable the automatic execution of operations when (and only when) all conditions are met, as they were initially encoded in the smart contract. All authorized parties can access the ledger to check which operations have been executed, and smart contracts to verify how they were programmed. This is a substantial confidence enhancer for all interested parties, from counterparties to transactions, business partners to regulators if they wish to use blockchain in their supervision missions.
- Liquidity. Tokenisation can boost - or even create - liquidity for some intrinsically illiquid assets. This can cover shares that are not traded on secondary markets, venture capital and real estate industries.
- Cyber-resilience. Distributed ledgers are the “single version of the truth” kept in a decentralized way so no central point of failure can be identified in the context of cyber-attacks. This is a very substantial benefit for crucial activities that financial ones are, even more when they pose a systemic risk to financial stability.

Question 56. Do you think that the use of DLT for the trading and post-trading of financial instruments poses more financial stability risks when compared to the traditional trading and post-trade architecture?

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

56.1 Please explain your reasoning for your answer to question 56:

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

At this stage of the development of the security token industry, there is no evidence that the use of DLT for the trading and post-trading of financial instruments poses more financial stability risks. As described above (see answer to question 55), blockchain should become a tool to mitigate some risks thanks to transparency, trustworthiness, cyber-resilience.

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

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

Yes. As described above (see answer to question 55), DLT and smart contracts will significantly impact the role and operation of trading venues and post-trade financial market infrastructures (CCPs, CSDs) thanks to the automation and integration of processes on blockchain, and gains in terms of transparency, reliability, liquidity and cyber-resilience.

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

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

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

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

A gradual regulatory approach in the areas of trading, post-trading and asset management concerning security tokens is the best one in order to determine necessary legal adjustments for security tokens based on guarantees brought by the technological features of DLT (in terms of efficiency, security, reliability, privacy, liquidity, etc) and adapt rules, either because they cannot prevail in security token markets or to

make them simpler thanks to blockchain benefits.

To that end, the guarantees brought by crypto-assets' technological specificities must be carefully defined in order to lay the foundations of such legal adjustments.

To conduct such analysis, ADAN agrees with and supports the French financial regulator's approach to create a "digital laboratory at European level allowing the national competent authorities to remove, in return for appropriate guaranties, certain requirements imposed by European regulations and identified as incompatible with the blockchain environment, provided that the entity benefiting from this exemption respects the key principles of the regulations and that it is subject to increased surveillance by the national competent authority of the reference Member State".

In the short term, this would enable actors to get a greater clarity on the regulatory regime applying to them, this one being simpler and more proportionate. In the long run, regulators will get the necessary hindsight to adapt the current financial regulation to crypto-asset activities according to their specific opportunities and risks.

B. Assessment of legislation applying to 'security tokens'

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

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

1.1 Financial instruments

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

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

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

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

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

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

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

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

Building an EU regime requires convergence on the foundations of this regime. Among them, the first and most important one is the common understanding of the legal qualification of security tokens.

In line with our general recommendations, security tokens should be understood as crypto-assets that enter into the list of “financial instruments” as given by MiFID 2, annex I section C, and for some comply with the current definition of “transferable securities” under article 4.1.15 of MiFID 2. Crypto-assets that would exhibit “investment-type” characteristics but not formally fit into these two legal concepts should be considered as “tokens”/”(programmable) crypto-assets” and comply with the future regulatory regime applying to them. See our answers to questions asked in part II “Classification of crypto-assets”.

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

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

	1 (factor not relevant at all)	2	3	4	5 (very relevant factor)	Don’t know / no opinion / not relevant
Harmonise the definition of certain types of financial instruments in the EU	( )	( )	( )	( )	(●)	( )

Provide a definition of a security token at EU level	◉	○	○	○	○	○
Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token	○	○	○	○	◉	○

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

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

N/A

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

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

In line with our general recommendations, crypto-assets that qualify as existing legal instruments (such as financial instruments or transferable securities) should not be subject to another new qualification. To this end:

- There is no need for defining “security tokens”. However, in order to build some legal adjustments only applicable to them, such amendments should refer to their specific technical features. Investigating whether blockchain characteristics should be defined and/or listed might be questioned.
- A clear and homogeneous definition of “financial instruments” and the scope of assets that they cover is crucial across member States. The lack of convergence on the interpretation of financial instruments within the EU is not a specific problem to crypto-assets, then should be resolved in larger debates than the one about regulating crypto-assets.

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

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

	1				5	Don’t know /

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

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

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

N/ACrypto-assets that would exhibit “investment-type” characteristics but not formally fit into these two legal concepts should be considered as “tokens”/”(programmable) crypto-assets” and comply with the future regulatory regime applying to them. See our answers to questions asked in part II “Classification of crypto-assets”.

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

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

Crypto-assets that would exhibit “investment-type” characteristics but not formally fit into these two legal concepts should be considered as “tokens”/”(programmable) crypto-assets” and comply with the future regulatory regime applying to them. See our answers to questions asked in part II “Classification of crypto-assets”.

1.2. Investment firms

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

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

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

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

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

Question 63. Do you think that a clarification or a guidance on applicability of such rules and requirements would be appropriate for the market?

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

63.1 Please explain your reasoning for your answer to question 63:

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

In any aspect of regulation, legal certainty is favourable for the economic development of an industry. If at this time ADAN did not deeply analyse the whole regulatory package applying to investment firms and its appropriateness in the context of security tokens, it is likely that new actors on the market on financial instruments will have questions and expect clarifications from regulators. That is why this could be quite efficient to anticipate such questions.

1.3 Investment services and activities

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

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

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

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

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

The current list of investment services and activities established in MiFID II is not fully appropriate for security tokens.

One key problem is the structuration of secondary markets for security tokens. Not all exchanges can fit into one of the proposed services listed for operating a venue. Such is the case, firstly, of decentralized platforms. For all types of crypto-platforms, as participants are usually individuals, being qualified as regulated markets or multilateral trading facilities (MTF) or organised trading facilities (OTF) would create regulatory frictions considering the requirements that participants must be authorized entities.
Moreover, reception and transmission of orders and execution of orders do not illustrate the current functioning of crypto-assets markets. There is currently no use of such services and defining a regulatory framework for these providers should not be a priority.

Clarifying the list of investment services and activities that are relevant in the context of security tokens, and perhaps adding new ones to better reflect the reality behind the functioning of security token markets, could be one aspect of the work that the “digital laboratory at European level” promoted by the AMF should conduct.

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

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

1.4. Trading venues

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

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

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

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

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

1.5. Investor protection

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

Question 67. Do you think that current scope of investor protection rules (such as information documents and the suitability assessment) are

appropriate for security tokens? Please explain your reasoning.

5000 character(s) maximum

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

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

5000 character(s) maximum

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

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

5000 character(s) maximum

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

1.6. SME growth markets

To be registered as SME growth markets, MTFs need to comply with requirements under Article 33 (e.g. 50% of SME issuers, appropriate criteria for initial and ongoing admission, effective systems and controls to prevent and detect market abuse). SME growth markets focus on trading securities of SME issuers. The average number of transactions in SME securities is significantly lower than those with large capitalisation and therefore less dependent on low latency and high throughput. Since trading solutions on DLT often do not allow processing the amount of transactions typical for most liquid markets, the Commission is interested in gathering feedback on whether trading on DLT networks could offer cost efficiencies (e.g. lower costs of listing, lower transaction fees) or other benefits for SME Growth Markets that are not necessarily dependent on low latency and high throughput.

Question 70. Do you think that trading on DLT networks could offer cost efficiencies or other benefits for SME Growth Markets that do not require low latency and high throughput? Please explain your reasoning.

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

1.7. Systems resilience, circuit breakers and electronic trading

According to Article 48 of MiFID, Member States shall require a regulated market to have in place effective systems, procedures and arrangements to ensure its trading systems are resilient, have sufficient capacity and fully tested to ensure orderly trading and effective business continuity arrangements in case of system failure. Furthermore regulated markets that permits direct electronic access[30] shall have in place effective systems procedures and arrangements to ensure that members are only permitted to provide such services if they are investment firms authorised under MiFID II or credit institutions. The same requirements also apply to MTFs and OTFs according to Article 18(5). These requirements could be an issue for security tokens, considering that crypto-asset trading platforms typically provide direct access to retail investors.

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

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

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

1.8. Admission of financial instruments to trading

In accordance with Article 51 of MiFID, regulated markets must establish clear and transparent rules regarding the admission of financial instruments to trading as well as the conditions for suspension and removal. Those rules shall ensure that financial instruments admitted to trading on a regulated market are capable of being traded in a fair, orderly and efficient manner. Similar requirements apply to MTFs and OTFs according to Article 32. In short, MiFID lays down general principles that should be embedded in the venue's rules on admission to trading, whereas the specific rules are established by the venue itself. Since markets in security tokens are very much a developing phenomenon, there may be merit in reinforcing the legislative rules on admission to trading criteria for these assets.

Question 72. Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed? Please explain your reasoning.

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

Question 1.9 Access to a trading venues

In accordance with Article 53(3) and 19(2) of MiFID, RMs and MTFs may admit as members or participants only investment firms, credit institutions and other persons who are of sufficient good repute; (b) have a sufficient level of trading ability, competence and ability (c) have adequate organisational arrangements; (d) have sufficient resources for their role. In effect, this excludes retail clients from gaining direct access to trading venues. The reason for limiting this kind of participants in trading venues is to protect investors and ensure the proper functioning of the financial markets. However, these requirements might not be appropriate for the trading of security tokens as crypto-asset trading platforms allow clients, including retail investors, to have direct access without any intermediation.

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

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

Today, individuals are granted direct access to crypto-exchanges and are not intermediated by another actor. This allows faster transactions and cost-reduction (especially regarding brokerage fees).
When trading security tokens, the opportunity to involve the same intermediaries as for traditional financial markets should be questioned regarding the additional guarantees in terms of security, liquidity, transparency, etc. brought by DLT.
This risk-analysis could be one aspect of the work that the “digital laboratory at European level” promoted by the AMF should conduct.

1.10 Pre and post-transparency requirements

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

[31] MiFID II investment firms must take adequate measures to obtain the best possible result when executing the client's orders. This obligation is referred to as the best execution obligation.

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

- Completely agree
- Rather agree
- Neutral

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

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

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

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

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

1.11. Transaction reporting and obligations to maintain records

In its Article 25 and 26, MiFIR sets out detailed reporting requirements for investment firms to report transactions to their competent authority. The operator of the trading venue is responsible for reporting the details of the transactions where the participants is not an investment firm. MiFIR also obliges investment firms or the operator of the trading venue to maintain records for five years. Provisions would apply to security tokens very similarly to traditional financial instruments. The availability of all information on financial instruments required for reporting purposes by the Level 2 provisions could perhaps be an issue for security tokens (e.g. ISIN codes are mandatory).

Question 76. Would you see any particular issue (legal, operational) in applying these requirement to security tokens which should be addressed? Please explain your reasoning.

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

2. Market Abuse Regulation (MAR)

MAR establishes a comprehensive legislative framework at EU level aimed at protecting market integrity. It does so by establishing rules around prevention, detection and reporting of market abuse. The types of market abuse prohibited in MAR are insider dealing, unlawful disclosure of inside information and market manipulation. The proper application of the MAR framework is very important for guaranteeing an appropriate level of integrity and investor protection in the context of trading in security tokens.

Security tokens are covered by the MAR framework where they fall within the scope of that regulation, as determined by its Article 2. Broadly speaking, this means that all transactions in security tokens admitted to trading or traded on a trading venue (under MiFID Article 4(1)(24) 'trading venue' means a regulated market (RM), a Multilateral Trading Facility (MTF) or an Organised Trading Facility (OTF')) are captured by its provisions, regardless of whether transactions or orders in those tokens take place on a trading venue or are conducted over-the-counter (OTC).

2.1. Insider dealing

Pursuant to Article 8 of MAR, insider dealing arises where a person possesses inside information and uses that information by acquiring or disposing of, for its own account or for the account of a third party, directly or indirectly, financial instruments to which that information relates. In the context of security tokens, it might be the case that new actors, such as miners or wallet providers, hold new forms of inside information and use it to commit market abuse. In this regard, it should be noted that Article 8(4) of MAR contains a catch-all provision applying the notion of insider dealing to all persons who possess inside information other than in circumstances specified elsewhere in the provision.

Question 77. Do you think that the current scope of Article 8 of MAR on insider dealing is appropriate to cover all cases of insider dealing for security tokens?
Please explain your reasoning.

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

2.2. Market manipulation

In its Article 12(1)(a), MAR defines market manipulation primarily as covering those transactions and orders which (i) give false or misleading signals about the volume or price of financial instruments or (ii) secure the price of a financial instrument at an abnormal or artificial level. Additional instances of market manipulation are described in paragraphs (b) to (d) of Article 12(1) of MAR.

Since security tokens and blockchain technology used for transacting in security tokens differ from how trading of traditional financial instruments on existing trading infrastructure is conducted, it might be possible for novel types of market manipulation to arise that MAR does not currently address. Finally, there could be cases where a certain financial instrument is covered by MAR but a related unregulated crypto-asset is not in scope of the market abuse framework. Where there would be a correlation in values of such two instruments, it would also be conceivable to influence the price or value of one through manipulative trading activity of the other.

Question 78. Do you think that the notion of market manipulation as defined in Article 12 of MAR is sufficiently wide to cover instances of market manipulation of security tokens? Please explain your reasoning.

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

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

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

3. Short Selling Regulation (SSR)

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

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

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

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

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

80.1 Is there any other issue that would prevent effectively applying SSR to security tokens? Please specify which one(s) and explain your reasoning:

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

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

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

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

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

4. Prospectus Regulation (PR)

The Prospectus Regulation establishes a harmonised set of rules at EU level about the drawing up, structure and oversight of the prospectus, which is a legal document accompanying an offer of securities to the public and/or an admission to trading on a regulated market. The prospectus describes a company's main line of business, its finances, its shareholding structure and the securities that are being offered and/or admitted to trading on a regulated market. It contains the information an investor needs before making a decision whether to invest in the company's securities.

4.1. Scope and exemptions

With the exception of out of scope situations and exemptions (Article 1(2) and (3)), the PR requires the publication of a prospectus before an offer to the public or an admission to trading on a regulated market (situated or operating within a Member State) of transferable securities as defined in MiFID II. The definition of 'offer of securities to the public' laid down in Article 2(d) of the PR is very broad and should encompass offers (e.g. STOs) and advertisement relating to security tokens. If security tokens are offered to the public or admitted to trading on a regulated market, a prospectus would always be required unless one of the exemptions for offers to the public under Article 1(4) or for admission to trading on a RM under Article 1(5) applies.

Question 82. Do you consider that different or additional exemptions should apply to security tokens other than the ones laid down in Article 1(4) and Article 1(5) of PR?

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

82.1 Please explain your reasoning for your answer to question 82:

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

4.2. The drawing up of the prospectus

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

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

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

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

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

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

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

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

The content of the prospectus should be adapted to the specificities of security tokens.
On the one hand, under the current legislation, some crucial information is missing to enable potential subscribers to make informed decisions. On the other hand, parts of the content of the prospectus is also relevant for security tokens. That is why a "building block approach" seems the most effective approach.
Among information that we consider that potential subscribers of security tokens should be aware in order to better realize the characteristics and risks of an STO, might appear in the prospectus those that relate to: the underlying technology and its risks, the characteristics and the rights attached to the tokens, as well as details in the event of subscription of crypto-assets (instead of or in addition to a traditional subscription in current currency legal).
First, if security tokens are financial instruments within the meaning of MiFID II, the fundamental difference lies in the blockchain technology on which they are based. This is why it seems logical to specify its specific characteristics and risks. The issuer should thus describe the underlying technologies used, and the technical specifications such as architecture, protocol, and standards they could have used. Complete information would also go through the detailed description of the general and specific technological risks of the underlying technology(ies) selected by the issuer, and through the presentation of the risks linked to asset transfers, cyber-criminality and possible blockchain vulnerabilities. More "technologically savvy" subscribers may wish to consult the computer program used for the functional issue / description, or even its certification by a competent third party when the issuer requests it.
Compared to a traditional initial public offering, STOs have specific characteristics and rights attached to security tokens which are specific to crypto-assets. On the one hand, the technology on which the tokens will be registered and, if applicable, the technology on which the issuer intends to migrate the tokens after issuance should be presented. On the other hand, the modalities of transmission of the tokens and, where applicable, the intention of the issuer to request their admission on an exchange platform.
Regarding this last point, the information currently requested under the prospectus should be adapted to the reality of security tokens. Indeed, article 7.7.b of the Prospectus Regulation requires the issuer to indicate

whether the financial tokens will be traded on an organized market, namely a regulated market or a multilateral trading facility (MTF). Thus, the text as it stands does not take into account the other possible negotiation methods for digital assets, such as the use of a decentralized platform or the peer-to-peer exchange of security tokens.
Finally, if applicable, the prospectus should provide details in the event of subscription to digital assets (cryptocurrencies or stablecoins), which issuers of financial tokens can request in place of or in addition to a traditional subscription in legal tender currency. Then, the terms of payment-delivery could be clarified, as well as the mechanisms of storage of the digital assets collected: the means of collection and monitoring of the assets, the description of the systems of follow-up and safeguard of the assets received, or even the policy currency risk management and the conditions under which the issuer intends to convert crypto-assets into foreign currency. Also, the process of possible return of the assets to their subscribers should be presented, clarifying the repayment terms and the device for managing the exchange risk at the time of this repayment.

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

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

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

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

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

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

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

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

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

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

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

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

As described above (see answer to question 83), STOs unveil specific risks that are not covered in the current texts and should be mentioned in the prospectus.

ADAN does not know about ESMA's guidelines on risk factors, but as STOs pose new risks that were not treated in the Prospectus Regulation, it is likely that they are neither in these guidelines.

5. Central Securities Depositories Regulation (CSDR)

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

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

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

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

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

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

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

Whether records on a DLT platform can be qualified as securities accounts and what can be qualified as credits and debits to such an account;						
Definition of ‘book-entry form’ and ‘dematerialised form						
Definition of settlement (meaning the completion of a securities transaction where it is concluded with the aim of discharging the obligations of the parties to that transaction through the transfer of cash or securities, or both);						
What could constitute delivery versus payment in a DLT network, considering that the cash leg is not processed in the network						
What entity could qualify as a settlement internaliser						

88.1 Is there any other particular issue with applying the following definitions in a DLT environment Please specify which one(s) and explain your reasoning:

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

88.2 Please explain your reasoning for your answer to question 88:

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

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

- Yes

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

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

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

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

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

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

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

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

						strong concern
Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system	○	○	○	○	○	○
Rules on measures to prevent settlement fails	○	○	○	○	○	○
Organisational requirements for CSDs	○	○	○	○	○	○
Rules on outsourcing of services or activities to a third party	○	○	○	○	○	○
Rules on communication procedures with market participants and other market infrastructures	○	○	○	○	○	○
Rules on the protection of securities of participants and those of their clients	○	○	○	○	○	○
Rules regarding the integrity of the issue and appropriate reconciliation measures	○	○	○	○	○	○
Rules on cash settlement	○	○	○	○	○	○
Rules on requirements for participation	○	○	○	○	○	○
Rules on requirements for CSD links	○	○	○	○	○	○
Rules on access between CSDs and access between a CSD and another market infrastructure	○	○	○	○	○	○

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

5000 character(s) maximum

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

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

5000 character(s) maximum

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

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

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

In France, the two “Blockchain decrees” constituted a first step towards tokenization of financial assets by allowing the use of distributed ledgers for the issuance, registration, and transfer of some securities instead of traditional securities accounts (giving the samel legal effects, such as the transfer of ownership):
- The “Blockchain decree” No. 2016-520: for “mini-bons” that is a class of short-term debt instrument dedicated to the financing of SMEs;
- The “Blockchain decree” No. 2017-1674: for securities that are not admitted to the operation of a Central Securities Depository (non-listed Equity, transferable debt securities, shares of collective investment undertakings)

To this end, they introduced a legal concept for distributed ledgers : “shared electronic recording system” (DEEP in French).

6. Settlement Finality Directive (SFD)

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

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

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

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

						Don’t know /

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

93.1 Is there any other particular issue with applying the following definitions in the SFD or its transpositions into national law in a DLT environment? Please specify which one(s) and explain your reasoning:

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

93.2 Please explain your reasoning for your answer to question 93:

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

Question 94. SFD sets out rules on conflicts of laws. According to you, would there be a need for clarification when applying these rules in a DLT network (in particular with regard to the question according to which criteria the location of the register or account should be determined and thus which

Member State would be considered the Member State in which the register or account, where the relevant entries are made, is maintained)? Please explain your reasoning.

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

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

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

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

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

7. Financial Collateral Directive (FCD)

The Financial Collateral Directive aims to create a clear uniform EU legal framework for the use of securities, cash and credit claims as collateral in financial transactions. Financial collateral is the property provided by a borrower to a lender to minimise the risk of financial loss to the lender if the borrower fails to meet their financial obligations to the lender. DLT can present some challenges as regards the application of FCD. For instance, collateral that is provided without title transfer, i.e. pledge or other form of security financial collateral as defined in the FCD, needs to be enforceable in a distributed ledger[32].

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

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

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

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

97.1 Is there any other particular issue with applying the following definitions in the FCD or its transpositions into national law in a DLT environment? Please specify which one(s) and explain your reasoning:

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

97.2 Please explain your reasoning for your answer to question 97:

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

Question 98. FCD sets out rules on conflict of laws. Would you see any particular issue with applying these rules in a DLT network[32]?

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

Question 99. In your Member State, what requirements does your national law establish for those cases which are outside the scope of the FCD rules on conflicts of laws?

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

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

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

8. European Markets Infrastructure Regulation (EMIR)

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

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

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

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

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

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

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

Security tokens do not need central clearing. As they are programmable, they could integrate encoded conditions to prevent from the counterparty risks that clearing arrangements aim at managing.

Avoiding the use of central clearing could be a good way of modernizing market infrastructure, as clearing houses are often suspected of becoming "too big to fail" entities due to the increasing role that they have since the 2008 crisis and the strengthening of the regulation of derivatives.

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

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

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

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

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

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

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

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

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

For any possible uncertainty, clarifications will always be expected by actors at one time of their development. If ADAN did not deeply investigate this specific question, as long as no legal provisions prevent from it and no studies concluded that this could pose more risk for investors and financial stability, we think that a positive clarification that DLT solutions including permissioned blockchain can be used within CCPs or TRs should be formalised by authorities.

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

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

9. The Alternative Investment Fund Directive

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

The following questions seek stakeholders' views on whether and to what extent the application of AIFMD to tokens could raise some challenges. For instance, AIFMD sets out an explicit obligation to appoint a depositary for each AIF. Fulfilling this requirement is a part of the AIFM authorisation and operation. The assets of the AIF shall be entrusted to

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

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

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

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

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

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

105.2 Please explain your reasoning for your answer to question 105:

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

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

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

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

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

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

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

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

	1 (not suited)	2	3	4	5 (very suited)	Don't know / no opinion / very suited
Provisions of the UCITS Directive pertaining to the eligibility of assets, including cases where such provisions are applied in conjunction with the notion "financial instrument" and/or "transferable security"	○	○	○	○	○	○
Rules set out in the UCITS Directive pertaining to the valuation of assets and the rules for calculating the sale or issue price and the repurchase or redemption price of the units of a UCITS, including where such rules are laid down in the applicable national law, in the fund rules or in the instruments of incorporation of the investment company;	○	○	○	○	○	○
UCITS Directive rules on the arrangements for the identification, management and monitoring of the conflicts of interest, including between the management company and its clients, between two of its clients, between one of its clients and a UCITS, or between two -UCITS;	○	○	○	○	○	○
UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;	○	○	○	○	○	○
Disclosure and reporting requirements set out in the UCITS Directive.	○	○	○	○	○	○

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

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

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

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

11. Other final comments and questions as regards tokens

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

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

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

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

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

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.

The “digital laboratory at European level” advocated by the AMF should allow creating a favourable environment for such solutions to develop and to prove their efficiency and safety.

Question 109. Which benefits and risks do you see in enabling trading or post-trading processes to develop on permissionless blockchains and decentralised platforms?

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

Permissionless blockchain and decentralized platforms allow for those specific benefits, that do not exists in centralized / private blockchains:

- auditability and transparency of the operations;
- probabilistic finality of the transactions, that cannot be altered after being executed;
- composability of the services, allowing the use of multiple building blocks built by other companies to develop a new product or a new service using securities.

The main risks associated with permissionless blockchains and decentralised platforms are:

- technical risks and limited upgradability of the services;
- privacy, as all the operations are public (although pseudonymous).

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

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

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

110.1 If you do think that the regulatory separation of trading and post-trading activities might prevent the development of alternative business models based on DLT that could more efficiently manage the trade life cycle, please identify the issues that should be addressed at EU level and the approach to address them. Please explain your reasoning.

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

As blockchain allows for atomicity of transactions, and therefore the realization in one computing operation of all the trades and the post-trade operations, the regulatory separation of those two functions could alter the interest of interesting new business models.

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

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

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

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

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

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

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

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

The two “Blockchain decrees” described above (see answer to question 92) do not cover security tokens that are admitted to trade to the operation of a Central Securities Depository, that is those that are tradeable on secondary markets.

C. Assessment of legislation for ‘e-money’ tokens

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

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

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

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

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

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

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

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

Question 114. Have you detected any issue in PSD2 which would constitute impediments to the effective functioning or use of payment transactions related to e-money token?

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

114.1 Please provide specific examples (PSD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application, ...) and explain your reasoning for your answer to question 114:

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

Question 115. In your view, do EMD2 or PSD2 require legal amendments and /or supervisory guidance (or other non-legislative actions) to ensure the effective functioning and use of e-money tokens?

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

115.1 Please provide specific examples and explain your reasoning for your answer to question 115:

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

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

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

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

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

116.1 Is there any other requirement under EMD2 that would be appropriate for "global stablecoins"? Please specify which one(s) and explain your reasoning:

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

116.2 Please explain your reasoning for your answer to question 116:

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

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

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

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

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

Additional information

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

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

Useful links

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

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

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

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

Contact

fisma-crypto-assets@ec.europa.eu