CONSULTATION DOCUMENT
On an EU framework for markets in crypto-assets

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

The views reflected on this consultation paper provide an identification on the approach the Commission services may take but do not constitute a final policy position or a formal proposal by the European Commission.
You are invited to reply by **19 March 2020** at the latest to the online questionnaire available on the following webpage:


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

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

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

INTRODUCTION:

1. Background for this public consultation

As stated by President von der Leyen in her political guidelines for the new Commission, it is crucial that Europe grasps all the potential of the digital age and strengthens its industry and innovation capacity, within safe and ethical boundaries. Digitalisation and new technologies are significantly transforming the European financial system and the way it provides financial services to Europe’s businesses and citizens. Almost two years after the Commission adopted the Fintech Action Plan in 2018¹, the actions set out in it have largely been implemented.

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

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

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

Crypto-assets are one of the major applications of blockchain for finance. Crypto-assets are commonly defined as a type of private assets that depend primarily on cryptography and distributed ledger technology as part of their inherent value⁴. 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 2009³. There are many ways to classify the different types of crypto assets⁴. 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

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
⁴ See: ESMA Securities and Markets Stakeholder Group, Advice to ESMA, October 2018
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. 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 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, 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, 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: (i) For crypto-assets that are covered by EU rules by virtue of qualifying as financial instruments under the Markets in financial instruments Directive or as electronic money under the Electronic Money Directive, 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

---

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.


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

8 G7 Working group on ‘Stablecoins’, Report on ‘Investigating the impact of global stablecoins’, October 2019

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

10 Market in Financial Instruments Directive (2014/65/EU)

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”\(^{12}\). Executive Vice-president Valdis Dombrovskis has also indicated his intention to propose a new legislation for a common EU approach on crypto-assets, including “stablecoins”. While acknowledging the risks they may present, the Commission and the Council have also jointly declared that they “are committed to put in place the framework that will harness the potential opportunities that some crypto-assets may offer”\(^{13}\).

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

In this context and in line with Better Regulation principles\(^{14}\), the Commission is inviting stakeholders to express their views on the best way to enable the development of a sustainable ecosystem for crypto-assets while addressing the major risks they raise. This consultation document contains four separate sections.

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

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

- **The second section seeks feedback from stakeholders on whether and how to classify crypto-assets.** This section concerns both crypto-assets that fall under existing EU legislation (those that qualify as ‘financial instruments’ under MiFID II and those qualifying as ‘e-money’ under EMD2) and those that do not.

- **The third section invites views on the latter, i.e. crypto-assets that currently fall outside the scope of the EU financial services legislation.** In that first section, the term ‘crypto-assets’ is used to designate all the crypto-assets that are not regulated at EU level\(^{15}\). At certain point in that part, the public consultation makes further distinction among those crypto-assets and uses the terms ‘payment tokens’, “stablecoins” ‘utility tokens’, ‘investment tokens’. The aim of these questions is to determine whether an EU regulatory framework for those crypto-assets is needed. The replies will also help identify the main risks raised by unregulated 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

---

\(^{12}\) *Mission letter of President-elect Von der Leyen to Vice-President Dombrovskis*, 10 September 2019

\(^{13}\) *Joint Statement of the European Commission and Council on ‘stablecoins’,* 5 December 2019

\(^{14}\) *European Commission,* ‘Better Regulation: Why and How’

\(^{15}\) Those crypto-assets are currently unregulated at EU level, except those which qualify as ‘virtual currencies’ under the AML/CFT framework (see section I.C. of this document).
called ‘security tokens’ and ‘e-money tokens’. Responses will allow the Commission to assess the impact of possible changes to EU legislation (such as the Prospectus Regulation\textsuperscript{16}, MIFID II, the Central Securities Depositaries Regulation\textsuperscript{17}) on the basis of a preliminary screening and assessment carried out by the Commission services. This section is therefore narrowly framed around a number of well-defined issues related to specific pieces of EU legislation. Stakeholders are also invited to highlight any further regulatory impediments to the use of DLT in the financial services.

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

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

This consultation is open until \textbf{19 March 2020}.

\textbf{PUBLIC CONSULTATION}

\textbf{I. Questions for the general public}

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

1) \textbf{Have you ever held crypto-assets?}
   - Yes
   - No

2) \textbf{If you held crypto-assets, what was your experience?} [Insert text box]

   2.1. \textbf{Was it simple and straightforward to buy them?}
       - simple
       - neither easy nor hard
       - complex

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

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

   2.4. \textbf{Did you hold the crypto-assets with a custodial wallet provider?}
       - Yes
       - No

\textsuperscript{16} \textbf{Prospectus Regulation} (2017/1129/EU)
\textsuperscript{17} \textbf{Central Securities Depositaries Regulation} (909/2014/EU)
2.5. What type of crypto-assets, have you held?

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

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

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

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

- Yes
- No

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

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

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

4) If yes, in what timeframe?

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

II. Classification of crypto-assets\textsuperscript{18}

There is not a single widely agreed definition of ‘crypto-asset’. In this public consultation, a crypto-asset is considered as “a digital asset that may depend on cryptography and exists on a distributed ledger”. This notion is therefore narrower than the notion of ‘digital asset’\textsuperscript{19} that could cover the digital representation of other assets (such as scriptural money).

While there is a wide variety of crypto-assets in the market, there is no commonly accepted way 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

\textsuperscript{18} This section concerns both crypto-assets that fall under existing EU legislation (those that qualify as ‘financial instruments’ under MiFID II and those qualifying as ‘e-money’ under EMD2) and those falling outside. \textsuperscript{19} Strictly speaking, a digital asset is any text or media that is formatted into a binary source and includes the right to use it.
understand the obligations they are subject to. Therefore, a categorisation of crypto-assets is a key element to determine whether crypto-assets fall within the current perimeter of EU financial services legislation.

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

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

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

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

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

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

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

Defining crypto-assets in a broad sense is something useful at EU level, especially because we might encounter an issue of level playing field between entities regulated at national level and those who are not subject to any regulation in their home country.

Moving towards a classification of the different assets (e.g. utility tokens”, “security tokens”, “payment tokens”, “stablecoins”, “global stablecoins” etc.) would allow providing a clear picture of crypto-assets and define crypto-assets according to their respective economic functions. This classification, which is not an objective per se, would help drawing a line on the nature of the assets and of their legal qualification. This would help at highlighting the risks (micro or macro) triggered by their usage and assess whether regulation is appropriate.

As it might appear premature at this stage to give a precise classification of crypto-assets, we therefore express a preference for adopting a relatively broad and open set of definitions in order to capture all emerging crypto-asset types since crypto-assets represent a particularly moving market.

At this stage, we consider that these two key distinctions should be taken into due consideration:
distinction between crypto-assets that are qualified as financial instruments and crypto-assets that do not fall within the definition of a financial instrument;

distinction between crypto-assets that are qualified as electronic money and those which do not. We believe it is important to keep the electronic money regime, which is relevant and should not be undermined by a new regulation. However, it would be useful to work on the articulation between the different regimes.

We are in favor of an appropriate supervision and risk management, via a legislative tool to be adopted by the European Union (the best would be a regulation, or at least a directive); otherwise, we might encounter an issue of level playing field between entities regulated at national level and those who are not subject to any regulation in their home country.

Banque de France and ACPR are of the opinion that clarity on the legal qualification, provided that such a classification is set in light of the objective of capturing all emerging crypto-asset types, does not hamper innovation but rather mitigate risks for consumers and investors. This is in particular true for global stablecoins.

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).

This classification should first define the notion of crypto-assets, and then define the different types of crypto-assets (coins, tokens) and their subdivisions (under the category of "tokens", there are “utility tokens”, security tokens” etc. and under the category of coins there are “stablecoins” for example. The European Union could draw from the French legislation. The PACTE bill n°2019-486 of the 22nd of May 2019 introduced articles L.54-10-1 and following of the Monetary and Financial Code defining the notions of crypto-assets, tokens, and the equivalent of coins: " les actifs numériques comprennent : 1° Les jetons mentionnés à l’article L. 552-2, à l’exclusion de ceux remplissant les caractéristiques des instruments financiers mentionnés à l’article L. 211-1 et des bons de caisse mentionnés à l’article L. 223-1 ; 2° Toute représentation numérique d’une valeur qui n’est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n’est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d’une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d’échange et qui peut être transférée, stockée ou échangée électroniquement. »

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

8.1 If you do agree that any EU classification of crypto-assets should make a distinction between “payment tokens”, “investment tokens” “utility tokens” and “hybrid tokens”, please indicate if any further subclassification would be necessary:

For the reasons explained for question #6, Banque de France and ACPR are in favor of a classification (e.g. utility tokens”, “security tokens”, “payment tokens”, “stablecoins”, “global stablecoins” etc.) that would allow providing a clear picture of crypto-assets and define crypto-assets according to their respective economic functions.
At this occasion, we do reiterate that crypto-assets have unique financial, monetary and technical features which set them apart from the currencies and payment instruments issued by financial institutions and central banks. No crypto-asset should be qualified as a means of payment and be considered as monetary value, as their value and existence is subject to contractual clauses.

Looking at a possible classification depending of the economic functions crypto-assets do fulfill, two types of crypto-assets could possibly be considered:

- Crypto-assets issued through an initial coin offering could be qualified as ‘tokens’. These tokens could be defined as ‘any intangible asset encompassing in a digital format one or several rights which can be issued, stored, put in custody or transferred via a distributed ledger technology allowing to identify directly or indirectly the owner of the asset’. Consequently, such a qualification could encompass all forms of tokens issued through an ICO such as utility tokens granting their user a right over a good or service or as a security token detained by users for investment purposes;

- Alternatively, crypto-assets not fitting into the token qualification could fall into a larger qualification where crypto-assets not issued through an initial coin offering could fit into (bitcoins, ether, ripple…). This larger category of crypto-assets could be defined as ‘any digital representation of value’ and include any crypto-asset meeting the following cumulative criteria:
  - The crypto-asset must not be issued or backed by a central bank or a public authority;
  - The crypto-asset is not necessarily tied to a fiat currency;
  - The crypto-asset does not possess the legal status of a fiat currency;
  - The crypto-asset is accepted by individuals or firms as a means of exchange;
  - The crypto-asset may be transferred, stored or digitally traded.

Lastly, it would be also useful to have specific provisions on ‘security tokens’ consistent with Regulation (EU) 909/2014 concerning central securities depositories.

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

Separate definitions are only needed if the risks they imply need to be addressed differently/separately.
The Deposit Guarantee Scheme Directive\textsuperscript{20} (DGSD) aims to harmonise depositor protection within the European Union and includes a definition of what constitutes a bank ‘deposit’. Beyond the qualification of some crypto-assets as ‘e-money tokens’ and ‘security tokens’, the Commission seeks feedback from stakeholders on whether other crypto-assets could be considered as a bank ‘deposit’ under EU law.

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

Since there should be no confusion between official money benefitting from legal tender on the one hand and crypto-assets on the other hand, crypto-assets should not be considered as bank deposits under EU law. These assets have a risk profile different from deposits and could endanger the DGS.

Article 2.3 of the DGSD defines a deposit as ‘a credit balance which results from funds left in account (…) which a credit institution is required to repay under the legal and contractual conditions applicable (…)’. Under French law, deposits are defined as ‘funds redeemable to the public’ (article L.312-2 of the French monetary and financial code [French MFC]). Repaying funds to the public is considered as a banking operation (article L.311-1 of the French MFC). These funds are collected from a third party, most notably as in the form of deposits. Credit institutions collecting the deposits are entitled to use them for their own account but are required to redeem them to the public. These activities may only be carried out by credit institutions (articles L.511-1 and L.511-5 of the French MFC).

Therefore, we believe that holding crypto-assets as deposits would lead to enlarging the number of financial intermediaries allowed to collect and redeem funds to the public, and would make crypto-assets eligible to the deposit guarantee schemes. This change would blur the lines between the different financial intermediaries’ authorized activities and would imply that bank failure with “crypto deposits” may be finally paid by taxpayer funds. In our opinion, crypto-assets should not be assimilated to deposits since they do not entail the same legal obligations for service providers. Whereas credit institutions are contractually and legally required to redeem deposits to deposit holders, crypto-asset issuers are under no legal requirement to repay funds in fiat currency to crypto-assets holders although there may exist a contractual arrangement between them requiring them to.

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\textsuperscript{21} (A.) and on the risks presented by some service providers related to crypto-assets and the best way to mitigate them (B.). This section also raises horizontal questions concerning market integrity, Anti-Money laundering (AML) and Combatting the Financing of Terrorism (CFT), consumer/investor protection and the supervision and oversight of the crypto-asset sector (C.).

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

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

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

<table>
<thead>
<tr>
<th>Benefit</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Issuance of utility tokens as an alternative funding source for start-ups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cheap, fast and swift payment instrument</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Enhanced financial inclusion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Benefit</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto-assets as a new investment opportunity for investors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Improved transparency and traceability of transactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Enhanced innovation and competition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Improved liquidity and tradability of tokenised ‘assets’</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Enhanced operational resilience (including cyber resilience)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Security and management of personal data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Possibility of using tokenisation to coordinate social innovation or decentralised governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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. 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. 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, this might change in the future.

11) In your opinion, what are the most important risks related to crypto-assets? Please rate each proposal from 1 to 5, 1 standing for "not important at all" and 5 for "very important". [insert text box]
<table>
<thead>
<tr>
<th>Fraudulent activities</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market integrity (e.g. price, volume manipulation...)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investor/consumer protection</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-money laundering and CFT issues</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data protection issues</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competition issues</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber security and operational risks</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Taxation issues</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energy consumption entailed in crypto-asset activities</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial stability</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monetary sovereignty/monetary policy transmission</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

22 ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019
23 For example when established market participants operate on private permission-based DLT, this could create entry barriers.
24 FSB Chair’s letter to G20 Finance Ministers and Central Bank Governors, Financial Stability Board, 2018

“Stablecoins” are a relatively new form of payment tokens whose price is meant to remain stable through time. Those “stablecoins” are typically asset-backed by real assets or funds (such as short-term government bonds, fiat currency, commodities, real estate, securities…) or by other crypto-assets. They can also take the form of algorithmic “stablecoins” (with algorithm being used as a way to stabilise volatility in the value of the coin). While some of these “stablecoins” can qualify as ‘financial instruments’ under MiFID II or as e-money under EMD2, others may fall outside the scope of EU regulation. A recent G7 report on ‘investigating the impact of global stablecoins’25 analysed “stablecoins” backed by a reserve of real assets or funds, some of which being sponsored by large technology or financial firms with a large customer base. The report underlines that “stablecoins” that have the potential to reach a global scale (the so-called “global stablecoins”) are likely to raise additional challenges in terms of financial stability, monetary policy transmission and monetary sovereignty, among others. Users of “stablecoins” could in principle be exposed, among others, to liquidity risk (it may take time to cash in such a “stablecoin”), counterparty credit risk (issuer may default) and market risk (if assets held by issuer to back the “stablecoin” lose value).

12) In our view, what are the benefits of “stablecoins” and “global stablecoins”? Please explain your reasoning (if needed).

Stablecoins, because of their expected relatively stable value denominated compared to other types of crypto-assets, could be widely used as a means of payment. They could also facilitate cross-border payments and increase financial inclusion, in particular if they manage to have a global reach.

It is nevertheless quite clear that crypto-assets undergoing technical and economic trials bring about not only opportunities to improve our payment systems but also material risks which on the contrary might weaken them if unaddressed, both from an efficiency perspective and a safety perspective through the introduction of new sources of fragmentation, instability and fraud.

In this respect, Banque de France reiterates that the central bank money plays the role of an anchor into the payment landscape as it is the sole settlement asset with legal tender status. This core
feature which have served well the public interest of financial and monetary stability should be preserved, together with the advantages of multiple issuers of settlement assets in providing innovative, efficient and safe means of payment.

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

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

Please explain in your answer potential differences in terms of risks between “stablecoins” and “global stablecoins” (if needed).

Distinction should be made between the risks associated with existing crypto-assets and the risks that would appear if crypto-assets, more likely stablecoins, reach global scale. In such a global use, the risks regarding financial stability, monetary sovereignty and monetary policy transmissions, and competition would be radically heightened, as outlined by the G7 report on global stablecoins (G7 report on global stablecoins of October 2019).

Global stablecoins (GSCs - e.g. those that reach global scale) could potentially affect financial stability by increasing fragilities in the conventional domestic currency financial sector and facilitating the cross-border transmission of shocks, and in the end, affect the real economy in multiple countries.

In terms of monetary policy, GSC could alter the implementation and transmission of monetary policies if they become a credible substitute for cash and bank deposits (which is not the case with existing crypto-currencies), particularly for emerging countries already suffering from partial dollarisation of their economies and for which the Libra could constitute a reserve of value seen as more stable. This also raises the question of the links between central banks and entities of this type. In addition to these considerations, there are also issues related to the strategic role of financial infrastructures, particularly payment infrastructures. GSC may also underline monetary sovereignty with people simply stop using their national currency and turning to this private currency as a new unit of account instead.

Global stablecoins are also likely to be issued by large incumbent global technology firms and therefore may arise risks similar to those of crypto-assets but on a different scale and thus exacerbate existing risks as well as create new risks in financial markets. For instance, network effect, market risk and liquidity risk of stablecoins is amplified in the case of global stablecoins. This may lead to providers (when it is identified) failing to internalise the risks from greater concentration and underinvesting in operational resilience.

Moreover, as the entities engaged in the ecosystem may be located in different jurisdictions and
due to the cross-border nature of SCs and GSCs issues pertaining to conflict of law can arise. This is especially true given that global stablecoins are more likely to be unable to enforce their rules and arrangements in all relevant jurisdictions due to their global scale and to the different legal qualifications existing in different jurisdictions. Due to its inherently cross-border nature, the Libra Proposal and other global stablecoins are likely to raise challenges in terms of supervision. Diverging legal qualifications in Europe may give rise to a risk of jurisdiction-shopping, and potentially a risk for a Member State to have a stable coin marketed in its jurisdiction through the passporting mechanism.

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


14) In your view, would a bespoke regime for crypto-assets (that are not currently covered by EU financial services legislation) enable a sustainable crypto-asset ecosystem in the EU (that could otherwise not emerge)?
   ▪ Yes
   ▪ No
   ▪ Don’t know/no opinion

Please explain your reasoning (if needed).

These new assets (and their operators) cannot being traded without being appropriately regulated considering the risks they imply and a regulation at national level seems to be improper to regulate assets, which have a global reach. There must be a level playing field in the European Union. Otherwise, we might assist to the emergence of various and very different regulatory regimes.

There is a need to create a bespoke regime at EU level for all crypto-assets that are not qualified as financial instruments, depending of their systemic impact. The objective is to have a sustainable, safe and sound crypto-asset ecosystem in the EU. Banque de France and ACPR are of the opinion that such a regime would offer the benefit of providing an increased level of protection for investors as well as legal clarity to the crypto-asset ecosystem. It would also take into account the specificities of the environment.

In that spirit, there is also a need to ensure a level-playing field between all assets. In our view, an optional regime only makes sense on a national basis in the absence of any EU regulation. Banque de France and ACPR are of opinion that any bespoke regime must be exclusively based on mandatory requirements, at EU level, whatever be the function and systemic feature of crypto-assets. A bespoke regime would allow to have a proportionate and progressive approach in a mandatory framework. In the same vein, such a regime must be framed by the current regulatory framework and international principles, such as the Principles for Market Infrastructures (PFMI) that ensure the markets and market infrastructures function properly on a day-to-day basis.

15) What is your experience (if any) as regards national regimes on crypto-assets?
   Please indicate which measures in these national laws are, in your view, an effective approach to crypto-assets regulation, which ones rather not.
Since the adoption of the PACTE bill on 22nd of May 2019, French law now defines as ‘digital assets’ two kinds of crypto-assets: ‘tokens’ issued through an initial coin offering (article L.54-10-1 1° of the French monetary and financial code [French MFC]) and ‘digital representations of value that may be used as a means of exchange’ (article L.54-10-1 2° of the French MFC). Additionally, French law lists five types of digital asset services, namely (i) custodial wallet services, (ii) selling and buying digital assets against fiat currency, (iii) trading digital assets against other digital assets, (iv) running an exchange platform and (v) providing investment services on digital assets (article L.54-10-2 French MFC).

The French national regime for digital assets service providers entails a registration requirement for custodians and for providers of services consisting in selling and buying digital assets against fiat currency (articles L.54-10-3 and L.54-10-4 French MFC). The French Financial Markets Authority (AMF) is the competent authority for this registration process. The French Prudential Control and Resolution Authority (ACPR) has to give its assent to the registration. Besides registration, French law grants digital asset service providers the opportunity to be authorized.

All registered crypto-asset service providers are subject to the following prudential rules (article L.54-10-3 of the French MFC):

- Fit and proper standards for the managers of a custodial wallet service providers;
- Shareholders possessing 25% of the capital or voting rights of the service provider or having control over the service provider must justify that they guarantee sound and prudent management of the service provider and that they possess the adequate respectability and experience required by their functions;
- Service providers must demonstrate that they set up an organization, processes and internal control policies enabling the service provider to comply with their obligations as regards money laundering and terrorism financing as well as asset freezing dispositions and the prohibition on funds being made available.

All licensed crypto-asset service providers are required to possess the following prudential requirements at all times (article L.54-10-5 of the French MFC):

- A professional indemnity insurance or own funds;
  - This professional indemnity insurance may not be inferior to 400,000 euros per claim and 800,000 euros per year. When the service provider is also a payment service providers, this amount may be no lesser than 400,000 euros and no higher than the maximum amount required by its payment services license (article 721-5 of the French Financial Markets Authority [AMF]'s general rules);
  - Alternatively, the equity must correspond to at least the highest amount of the amounts resulting from the following calculation methods:
    - the equity requirement based on fixed overheads;
    - the equity requirement based on minimum capital;
    - the equity requirement based on level of activity (instruction 2019-23 of the French AMF);
- Adequate security and internal control policies;
- A resilient and secure IT system;
- Internal processes suitable to manage conflict of interests.

Depending on the specificity of their activities, licensed crypto-assets service providers may
be subject to additional prudential requirements.

Moreover, French law now encompasses an initial coin offerings framework (article L. 552-1 of the French MFC). An issuer wishing to issue tokens to the public is now required to obtain a visa from the AMF. Before launching an ICO, the issuer is required to publish a white paper in order to inform the public of the tokens’ main characteristics (article L.552-4 of the French MFC).

On AML/CFT:
Because of their main features, crypto-assets are an easy way to launder money or to finance terrorism. That is why France has transposed 5AMLD with PACTE Law published on May 23rd 2019 to address ML-TF risks emerging from crypto-assets. Two types of virtual asset service providers must be registered and supervised: (i) providers engaged in exchange services between virtual currencies and fiat currencies and (ii) custodian wallet providers. Other entities involved in activities relating to virtual currencies which are not covered by the 5th AMLD (i.e. exchange between virtual assets, trading platform of virtual assets, provision of financial services related to virtual assets) can be licensed and supervised (optional licensing). Even if licensing isn’t mandatory, a majority of entities will apply for licensing since the activities that require registration and the activities for optional licensing are complementary. There are also strong incentives for licensing (i.e. right to hold an account with a credit institution, possible direct marketing of services, advertising,…). Registered and licensed VASPs must apply preventive measures, including CDD, STR and freezing action. Requiring that VASPs implement AML/CFT measures is an effective approach to crypto-assets regulations”.

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) [Insert text box]

A bespoke regime should at least be adopted for security tokens since, otherwise (i.e. without a legal framework authorising this form of securities) such assets would not be considered as securities. In that minimum scenario crypto-assets would be regulated the same way as corresponding “standard” assets.

Yet ideally, a bespoke European framework for crypto-assets and crypto-asset service providers should be extensive and subject all licensed crypto-asset service providers to all existing prudential requirements. Such requirements would include:

- Fit and proper standards;
- Minimum level of own funds;
- Internal control policies;
- Processes for managing effectively IT systems and conflict of interests;
- Policies to mitigate the money laundering and terrorism financing risk.

Requiring a minimum level of initial capital or a proper professional indemnity insurance and own funds seems of utmost importance. Indeed, crypto-asset service providers managing third parties’ funds when acquiring and executing payment transactions set up a minimum level of own funds that digital assets service providers should hold in order to protect the funds crypto-asset holders entrusted them with. Most notably, providers of crypto-assets used for payment purposes could be required to detain a minimum level of own funds depending on their level of
activity since crypto-asset service providers are hold sometimes funds on behalf of their clients. Alternatively, these service providers could be subject to a mandatory professional indemnity insurance or initial capital and own funds. This would align their regime with the one for payment institutions under the second Payment Services Directive (PSDII). Similarly, issuers of crypto-assets used for investment purposes could be required to possess a minimum level of own funds proportionate to their activity. This would align their regime with the regime for investment firms under the second Markets in Financial Instruments Directive (MiFID II). Crypto-assets exchange platforms could also be required to detain a minimum level of own funds as traditional trading venues are under MiFID II.

Additionally, coin issuers could be required to publish a whitepaper before launching an initial coin offering so as to inform investors on the tokens’ main characteristics. This requirement would put coin issuers on a level playing field with both equity security issuers and debt security issuers who have to publish a prospectus before launching an initial public offering under the third Prospectus regulation.

Eventually, in case funds are collected on behalf of third parties, it would be necessary to broaden the mechanism for protecting consumers’ funds by setting up a mechanism to confine funds on a segregated account held by a credit institution or any other device, which ensures maximum protection of consumers’ funds.

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

We support the current BCBS proposal on the prudential treatment of « high risk » crypto-assets as it is sufficiently cautious and conservative. In principle, for other kinds of crypto-assets, we also thinks that the prudential treatment will have to be specified once we will have a better understanding of their underlying risk.

We are also involved in ongoing work related to the same issue with the EBA, that will deserve to be reflected at the appropriate level in the EU prudential framework to ensure an harmonized application of these possible new rules (ie. preferably in Level 1 or, at a second best, in Level 2 texts).

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

Yes. As for any type of legislation, the existence of different national regimes may hamper the development of a common European market. For instance, diverging national regimes for crypto-assets and crypto-asset service providers may deter investors from investing in an initial coin offering organized in another European Union member state. Harmonizing national regimes for crypto-assets and crypto-asset service providers appears to us as necessary to create a common and mandatory European market for crypto-assets. A
European regulation might be better suited than a directive to establish a single unified regime for crypto-assets and crypto-asset service providers. Any new regulation must be framed by the current regulation in particular on listed securities. After the 2009 financial crisis, the EU regime has allowed an efficient and safe functioning of market infrastructures in compliance with the principles for market infrastructures (PFMI) established at international level (CPMI-IOSCO). In particular, financial markets rely on central bank money to work in safe and efficiency framework, which is provided in Europe through Target2-Securities.

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

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

26 See the discussion paper of the Basel Committee on Banking Supervision (BCBS) “Designing a prudential treatment for crypto-assets”, December 2019
19) Can you indicate the various types and the number of service providers related to crypto-assets (issuances of crypto-assets, exchanges, trading platforms, wallet providers...) in your jurisdiction? [Insert text box]

French law (article L.54-10-2 French MFC) define ten services providers related to crypto-assets and grouped in five classes:

(i) custodial wallet services on behalf of third parties defined either as custody services of digital assets or services to control means of access to digital assets (in order to hold, store or wire transfer digital assets);
(ii) selling and buying digital assets against fiat currency;
(iii) trading digital assets against other digital assets;
(iv) running an exchange platform;
(v) providing investment services on digital assets including:
   (v.i) the service of reception and transmission of orders for digital assets on behalf of third parties;
   (v.ii) the service of digital assets portfolios management on behalf of third parties;
   (v.iii) the advisory service to investors in digital assets;
   (v.iv) the digital assets underwriting service;
   (v.v) the service of placing on a firm commitment basis of digital assets;
   (v.vi) the service of placing without a firm commitment basis of digital assets.

See also question 15.

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. 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.

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

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

Please explain your reasoning (if needed).

Yes, we believe that the issuer of crypto-assets marketed to EU investors and/or consumers should be established or have a physical presence in the EU.
In order to ensure an appropriate level of protection, it appears difficult to effectively monitor an issuer of crypto-assets marketed to EU investors without a physical presence in the EU zone.

Special attention should thus be granted to avoid “letter-box entities” in the EU27. In France, the optional regulation of ICOs imposed to the issuer of crypto-assets willing to be granted with the visa to be incorporated as a legal entity established or registered in France. The effectiveness of regulators' power to impose sanctions as well as the respect of guarantees related to the procedure enabling the monitoring and safeguarding of the funds raised lead us to consider that a physical presence in EU would be needed in order to comply with substantive requirements as exposed in the ESMA's general opinion of May 2017).

Therefore, the creation of a single and harmonised crypto-asset market ensuring better protection for investors as well as enabling the development of crypto-asset activities would be a solution. Should there be a EU bespoke regime for crypto-assets, it should include a passporting regime authorising crypto-asset issuers and sponsors to market their crypto-assets in the EU27 zone.

Similarly, in addition to issuers of crypto-assets, the French legal regime also provides that crypto-assets service providers shall have a physical presence in France to be licensed. The French “PACTE” status creates a new category of regulated service providers: the DASP. The services related to digital assets include various kinds of traditional investment services, as soon as they are performed in relation to digital assets. As it would have been complicated to build a regime that favors French DASP and prevent foreign DAPS (not established in France) from targeting French investors, the French “PACTE” statute established an optional license system. Digital asset services may apply for an optional license by the AMF if they are established in France and if they comply with certain requirements in terms of organization, business conduct and financial resources. The rationale is the same as for ICO issuers: reliable actors will be encouraged to obtain the license as it will give them certain legal rights, help them market their services in France and reassure their customers. We believe that such optional regime should be encouraged at the EU level.

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

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

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

Banque de France believes that issuer of crypto-assets should be required to provide certain key information when issuing crypto-assets. As issuers are required to publish a prospectus when securities are offered to the public within an EU Member State (article 3.1 of the
Prospectus III Regulation), it would seem proportionate to request issuers to publish a whitepaper when tokens are offered to the public. This disclosure should happen before launching an initial coin offering. This choice has been made in France.

From the French perspective, an Initial Coin Offering (ICO) may be defined as a fundraising transaction carried out through a DLT resulting in a crypto-assets being offered to the public. These crypto-assets can then be used to obtain goods or services and do not fall within the definition of a financial instrument (this new regime is intended to capture ICOs and therefore does not apply to Security Token Offerings).

To that end, the French PACTE Law has introduced a specific regime for ICOs, offering the possibility to ICO issuers to apply for an optional approval given by the AMF.

To that end, the ICO’s issuer remains the entity that is responsible to provide accurate, clear and not misleading information. The issuer is supposed to be the entity that has control over the issuance and the crypto-assets.

When issuing an optional visa for a public offer of tokens, the AMF shall ensures that all issuers and their offers provide a certain number of minimum guarantees for better investor protection purpose:

The issuer of crypto-asset shall be incorporated as a legal entity established or registered in France;

Its information document (“white paper”) shall be drawn up in accordance with the requirements set out in the AMF General Regulation.

For this purpose, the information document shall be concise and comprehensible. It shall contain all information useful to the public regarding the offering and the token issuer to allow subscribers to make an investment decision and to understand risks relating to the offering. The information that it contains shall be accurate, clear and not misleading.

Article 712-2 of the AMF General Regulation (Book 7 – Title 1) defines the content of the information document and sets out the list of the information that shall be provided in the various sections. Annex II to Instruction AMF DOC-2019-06 sets out the content of these sections. Thus, the information document must contain certain key information such as:

- Information regarding the token issuer;
- Issuer’s project object of the offering;
- Rights and obligations attached to the tokens offered to the public;
- Risk factors (e.g. risks related to the project such as economic or technological);
- Characteristics of the initial coin offering (e.g. Number of tokens to be issued and already issued, soft/hard cap, Token issue price and explanation of the principles used to establish the price, etc.);
- The technical procedures of the token issue;
- Custody and refunding of the funds and digital assets collected via the initial coin offering;
- Systems to establish the identity of subscribers, AML/CFT and security systems;
- Applicable law and competent courts;
- Declaration of the persons responsible

Please note that, once the approval has been issued, the information document shall be made available to the general public by the token issuer on its website and published online by the
AMF. Any change or occurring of new element liable to have a significant influence on the investment decision of any potential subscriber between the issuance of approval and the close of the offering shall be described in an amended information document produced by the token issuer and approved by the AMF. Where applicable, the issuer shall inform investors on its website of the organisation of a secondary market.

After the approval is obtained, subscribers will be provided with annual information about the use of the assets collected by the issuer. The information document sets out the conditions under which this information is provided.

The issuer shall have implemented a mechanism during the offering to monitor and safeguard, the funds for the duration of the fund raising, in order to guarantee the proper allocation of funds to the planned project.

Such a mechanism can take different forms as long as they are detailed in the information document (e.g. traditional escrow agreement, a multi-signature system, or a smart contract based on DLT, etc.).

The issuer shall also have in place a system to ensure compliance with its obligations relating to anti-money laundering and terrorist financing (AML/CFT).

The token issuers concerned must comply with certain provisions regarding AML/CFT (Articles L. 561-2 et seq. of the Monetary and Financial Code). The AMF specifies that, in investigating approval applications, it will be especially attentive to the following points:

The establishment of a risk classification in order to determine the risk profile of each subscriber and the level of the vigilance measures to be complied with;
For any subscription for an amount exceeding a certain amount of money (e.g. €1,000) and for any subscription, even under this amount, which the issuer might suspect of contributing to AML/CFT, the implementation of vigilance measures allowing identification and verification of the subscribers’ identity:

- Identification of the subscriber, involving gathering the following identity information (e.g. family name date and place of birth; and for a legal entity: legal form, name, registration number and head office address);
- Identity check, involving gathering any written documents of a conclusive nature (e.g. official identity document; for a legal entity: any deed or excerpt from an official register);
- Internal procedures making it possible to determine the profile of the relationship established with the subscriber and to manage the identified risks.
- Internal control system allowing the issuer to check, according to a predefined system, the orderly functioning of the internal procedures throughout the offer period.
- Finally issuers are also subject to Tracfin reporting and information obligations listed in Articles L. 561-15 et seq. of the Monetary and Financial Code and must appoint a Tracfin reporter in their organisation for this purpose.

For more information on the French ICO regime click here.
22) If a requirement to provide the information on the offers of crypto-assets is imposed on their issuer/sponsor, would you see a need to clarify the interaction with existing pieces of legislation that lay down information requirements (to the extent that those rules apply to the offers of certain crypto-assets, such as utility and/or payment tokens)? Please rate each proposal from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant". [insert text box]

<table>
<thead>
<tr>
<th>Proposal</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Consumer Rights Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>The E-Commerce Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>The EU Distance Marketing of Consumer Financial Services Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

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

Under French law, rules on the publication of a prospectus are listed in the French monetary and financial code (French MFC). Such rules are not present in the French consuming code.

Consequently, we have no opinion on the need to clarify the interaction between a prospective obligation on crypto-assets' issuers or sponsors to issue a prospectus and the existing European legislation on consumer rights (e.g. Consumer Rights Directive, E-Commerce Directive and Distance Marketing of Consumer Financial Services Directive).

Alternatively, we could clarify the interaction between a prospective obligation on crypto-assets' issuers or sponsors to issue a prospectus and the existing European legislation on consumer rights (e.g. Consumer Rights Directive, E-Commerce Directive and Distance Marketing of Consumer Financial Services Directive), particularly where an overlap of regimes is no longer required.

23) Beyond any potential obligation as regards the mandatory incorporation and the disclosure of information on the offer, should the crypto-asset issuer or sponsor be subject to other requirements? Please rate each proposal from 1 to 5, 1 standing for “completely irrelevant” and 5 for "highly relevant”.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The managers of the issuer or sponsor should be subject to fitness and probity standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Please explain your reasoning (if needed).

- The managers of the issuer or sponsor should be subject to fitness and probity standards
Highly relevant. As any person entrusted with the handling and/or investment of third parties’ funds, we consider that managers of all crypto-assets service providers are required to possess the necessary respectability and experience suitable to their functions, and most notably:

- Managers of service providers registered to hold crypto-assets into custody;
- Managers of service providers registered to trade crypto-assets against fiat currency;
- Managers of service providers licensed to trade crypto-assets against other digital assets;
- Managers of service providers licensed to run a crypto-asset exchange platform;
- Managers or service providers licensed to provide investment services on crypto-assets.

- The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions

Highly relevant. In our opinion, token issuers should be subject to the obligation to present clear and unambiguous content in any form of advertisement as well as in their white paper. The information provided should be exact, clear and non-misleading information.

- 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

Highly relevant. Under French law, issuers of financial securities are only required to provide information on the securities they offer in the form of a prospectus as well as in an accounting and financial report. This information is delivered to the public as well as to the French Financial Markets Authority (article L.451-1-2 of the French MFC). French law does not require issuers of financial securities to safeguard the funds collected on an escrow account or on a trust account.

We do not favour establishing a legal obligation requiring token issuers or sponsors to safeguard the funds collected on an escrow account or on a trust account.

1.2. Issuance of “stablecoins” backed by real assets

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

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

A stablecoin’s global systemic importance could be measured in terms of the impact that a stablecoin arrangement’s failure can have on the global financial system and wider economy. Given that a stablecoin may be used as a means of payment or store of value, and could be used in multiple jurisdictions, the criteria to be considered in determining a GSC would need to take into account the potential uses in multiple jurisdictions. Taking reference from existing approaches such as the criteria that are often considered in determining the need for or degree of regulation, supervision, and oversight of FMIs (PFMI, 2012), and global systemically important banks (BCBS, 2013), an approach for determining GSCs could include factors such as:

- Number and type of stablecoin users
- Number and value of transactions
- Size of reserve assets
- Value of stablecoins in circulation
- Potential substantial cross-border use in payments and remittances;
- Number of jurisdictions with stablecoin users
- Market share in each jurisdiction
- Redemption linked to a foreign currency or multiple currencies
- Interconnectedness with financial institutions
- Available alternatives to using the GSC as a means of payment at short notice
- Business, structural and operational complexity

25) To tackle the specific risks created by “stablecoins” and “global stablecoins”, what are the requirements that could be imposed on their issuers and/or the manager of the reserve? Please indicate for both “stablecoins” and “global stablecoins” if each is proposal is relevant (leave it blank if you have no opinion).

<table>
<thead>
<tr>
<th></th>
<th>“Stablecoins”</th>
<th>“Global stablecoins”</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Relevant</td>
<td>Not relevant</td>
</tr>
<tr>
<td>The reserve of assets should only be</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>invested in safe and liquid assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(such as fiat-currency, short term-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>government bonds…)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The issuer should contain the creation</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>of “stablecoins” so that it is</td>
<td></td>
<td></td>
</tr>
<tr>
<td>always lower or equal to the value of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the funds of the reserve</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The assets or funds of the reserve</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>should be segregated from the issuer'</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s balance sheet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The assets of the reserve should not be</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>be encumbered (i.e. not pledged as</td>
<td></td>
<td></td>
</tr>
<tr>
<td>collateral)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The issuer of the reserve should be subject to prudential requirements (including capital requirements) | X | X |
--- | --- | --- |
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating | X | X |
Obligation for the assets or funds to be held in custody with credit institutions in the EU | X | X |
Periodic independent auditing of the assets or funds held in the reserve | X | X |
The issuer should disclose information to the users on (i) how it intends to provide stability to the “stablecoins”, (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve | X | X |
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically | X | X |
Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer | X | X |
Other

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

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

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

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

Please explain your reasoning (if needed).

Regulation should be adapted to the risks faced by stablecoins, and differentiate, where necessary, to the final user: should it be financial institutions or individuals. However, if retail stablecoins a destined to be offered to financial institutions (instead of individuals) for retail
payment purposes, then differentiation in the regulatory approach might not be justified.

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 while others use simple and inexpensive technology.

27) In your opinion and beyond market integrity risks (see section III. C. 1. below), what are the main risks in relation to trading platforms of crypto-assets? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

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

<table>
<thead>
<tr>
<th>Risk</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absence of accountable entity in the EU</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of adequate governance arrangements, including operational resilience and ICT security</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Absence or inadequate segregation of assets held on the behalf of clients (e.g. for ‘centralised platforms’)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conflicts of interest arising from other activities</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Absence/inadequate recordkeeping of transactions</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Absence/inadequate complaints or redress procedures are in place</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bankruptcy of the trading platform</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lacks of resources to effectively conduct its activities</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Losses of users’ crypto-assets through theft or hacking (cyber risks)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of procedures to ensure fair and orderly trading</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to the trading platform is not provided in an undiscriminating way</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delays in the processing of transactions</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other see below</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

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

In addition to those risks, there are others specific to crypto-asset trading platforms, such as:
- In the case of transactions that are directly recorded on the blockchain, the immutable nature of the blockchain means all transactions are final. There is no legal recourse for stolen or lost funds, as technologically crypto assets cannot be recovered or frozen without forking the blockchain to reject the transactions, an operation that requires some consensus;

- In terms of clearing and settlement, as of today, as crypto assets exist within an unregulated space, clearing and settlement does not occur through traditional, regulated channels, resulting in clearing and settlement risks. Most platforms do not become the direct counterparty to every transaction not bearing much responsibility for what takes place on their platforms.

- The risk of unfairly treated hard fork: when the platforms hold assets on behalf of clients (so-called “centralised platforms”), if a hard fork happens on a blockchain, the client is supposed to get the benefit from the fork, getting the value of the assets of both branch of the chain. However, many platforms refuse to give back the assets of one branch to the clients, which is unfair and abusive. This is only possible because of the lack of regulation. In France, this risk is addressed thanks to an ad hoc regulation (article 722-1, 4° of AMF General Regulation).

Here is a precision about the third risk mentioned in the previous table: “Absence or inadequate segregation of assets held on behalf of clients”. We believe that segregation of assets held on behalf of clients with assets held for own account is important. However, we believe that segregation of assets held on behalf of clients with one another should not be mandatory for platforms, because such fine segregation may be very costly while being of low added-value in terms of investor protection.

In order to mitigate the above risks, any potential European regime for crypto-asset intermediaries should take into account a certain number of key provisions that would apply to crypto-asset trading platforms.

The PACTE law provides for a bespoke framework governing the activities of secondary market crypto-assets intermediaries called digital asset service providers (“DASP”). The PACTE law sets up an optional license for DASPs which are licensed and placed under the supervision of the AMF.

The optional license covers a wide range of activities, among which the management of a crypto-assets trading platform was considered as a priority for the need of regulation. This concerns the management of one or more digital asset trading platforms, within which multiple buying and selling interests expressed by third parties for digital assets in exchange for other digital assets or a currency that is legal tender can interact in such a way as to result in the conclusion of contracts.

Such DASP licensed for the provision of the service of management of a crypto-assets trading platform must comply with the following obligations, under the conditions and within the limits provided for by the General Regulation of the AMF (for more information click here):

- The persons who effectively manage the service and the natural persons who either own, directly or indirectly, more than 25% of the service provider’s share capital or voting rights shall provide evidence that they have the necessary good repute and competence to perform their duties;

- Operators of crypto-asset trading platform shall provide evidence that they have established an organization procedures and internal control system;

- Operators of crypto-asset trading platform shall lay down operating rules that needs to stipulate some key information such as:

  - the conditions of users’ access to the trading platform for digital assets and their obligations;

  - the list or categories of digital assets that can be traded on the platform;
- the operating conditions of the trading platform for digital assets in the event of the use of discretion in the execution of orders.
- the conditions in which the operator of the trading platform may use its own capital;
- the conditions for trading digital assets on the platform (e.g. procedures for matching buying and selling interests, types of orders that may be processed on the trading platform, rules that apply where an automated trading system is used by clients, information made public concerning buying and selling interests and the transactions performed, procedures for suspending trading or notifying users in the event of a malfunction or failure of the trading platform, etc.);
- the transaction settlement procedures;
- where applicable, the conditions of custody of clients' digital assets by the trading platform for digital assets.

- Operators of crypto-asset trading platform shall ensure fair and orderly trading;
- Operators of crypto-asset trading platform shall commit their own capital to the platforms that they manage only under the conditions and within the limits laid down in the General Regulation of the AMF;
- Operators of crypto-asset trading platform shall publish the details of the orders and the transactions concluded on their platforms.

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

<table>
<thead>
<tr>
<th>Requirement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trading platforms should have a physical presence in the EU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should segregate the assets of users from those held on own account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should be subject to rules on conflicts of interest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should be required to keep appropriate records of users’ transactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should have an adequate complaints handling and redress procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should be subject to prudential requirements (including capital requirements)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should have adequate rules to ensure fair and orderly trading</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should provide access to its services in an undiscriminating way</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Trading platforms should be responsible for screening crypto-assets against the risk of fraud

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

[Insert text box]

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.

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

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

---

32 Study from the European Parliament on “Cryptocurrencies and Blockchain”, July 2018
Please explain your reasoning (if needed). [Insert text box]

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

<table>
<thead>
<tr>
<th>Requirement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence/Absence of accountable entity in the EU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Exchanges should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchanges should segregate the assets of users from those held on own account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Exchanges should be subject to rules on conflicts of interest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Exchanges should be required to keep appropriate records of users' transactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Exchanges should have an adequate complaints handling and redress procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Exchanges should be subject to prudential requirements (including capital requirements)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchanges should be subject to advertising rules to avoid misleading marketing/promotions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Exchanges should be responsible for screening crypto-assets against the risk of fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

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

Following the categorization of the crypto-asset as defined in this consultation paper, we believe certain rules are more relevant a type of crypto-asset more than another. One example might be that an ‘investment token’ would bear added risk with regard to conflicts of interest, and from a consumer protection view, increased complexity with regard to misleading marketing promotions.

Other considerations should be taken into account for crypto-asset trading platform when they handle third parties’ funds. We favour requiring such service providers to hold a payment services provider license under the second Payment Services Directive (PSD2). This requirement would ensure that investors’ funds are protected on a segregated account in a credit institution.

Alternatively, a bespoke regime for crypto-asset trading platforms could be set up. We believe that such platforms should be subject to extensive prudential requirements and most notably:

- Fit and proper standards for the managers of a trading platform;
- Shareholders possessing 25% of the capital or voting rights of the service provider or having control over the service provider must justify that they guarantee sound and prudent management of the service provider and that they possess the adequate respectability and experience required by their functions;
Service providers must demonstrate that they set up an organization, processes and internal control policies enabling the service provider to comply with their obligations as regards money laundering and terrorism financing as well as asset freezing dispositions and the prohibition on funds being made available;

Service providers must ensure a fair and orderly negotiation;

They must not trade on their own account on the exchange;

They must publish the orders and transactions negotiated on the exchange.

4. Provision of custodial wallet services for crypto-assets

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

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

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

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

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

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

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

Please indicate if those requirements should be different depending on the type of crypto-assets kept in custody by the custodial wallet provider and explain your reasoning (if needed).

Since custodial wallet providers are handling third parties’ funds for investment purposes, we favor requiring such service providers to be subject to the following prudential requirements:

- Fit and proper standards for the managers of a custodial wallet service providers;
- Shareholders possessing 25% of the capital or voting rights of the service provider or having control over the service provider must justify that they guarantee sound and prudent management of the service provider and that they possess the adequate respectability and experience required by their functions;
- Service providers must demonstrate that they set up an organization, processes and internal control policies enabling the service provider to comply with their obligations as regards money laundering and terrorism financing as well as asset freezing dispositions and the prohibition on funds being made available.
33) Should custodial wallet providers be authorised to ensure the custody of all crypto-assets, including those that qualify as financial instruments under MiFID II (the so-called ‘security tokens’, see section IV of the public consultation) and those currently falling outside the scope of EU legislation?

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

Please explain your reasoning (if needed).

Custodial wallet service providers should only be authorized to ensure the custody of those crypto-assets not qualifying as financial instruments under annex I of the second Markets in Financial Instruments Directive (MiFID II). Under French law, tokens that possess the characteristics of financial instruments are qualified as financial instruments under article L.211-1 of the French monetary and financial code (MFC). Different types of authorisations may coexist (ex: distinction between security tokens and other crypto-assets). However all custodial wallet providers should be subject to an authorization procedure.

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

We believe that all crypto-asset service providers who manage funds on behalf of their clients should be required to abide by prudential requirements. If a service provider in the digital wallet ecosystem manages investors’ funds, then such a service provider should abide by prudential requirements.

5. Other service providers

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

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

<table>
<thead>
<tr>
<th>Service</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reception and transmission of orders in relation to crypto-assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Execution of orders on crypto-assets on behalf of clients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Crypto-assets portfolio management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Advice on the acquisition of crypto-assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Underwriting of crypto-assets on a firm commitment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Service Description</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placing crypto-assets on a firm commitment basis</td>
<td></td>
</tr>
<tr>
<td>Placing crypto-assets without a firm commitment basis</td>
<td></td>
</tr>
<tr>
<td>Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)</td>
<td>X</td>
</tr>
<tr>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)</td>
<td>X</td>
</tr>
<tr>
<td>Services provided by developers that are responsible for maintaining/updating the underlying protocol</td>
<td></td>
</tr>
<tr>
<td>Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)</td>
<td>X</td>
</tr>
<tr>
<td>Other services</td>
<td></td>
</tr>
</tbody>
</table>

Please illustrate your response, by underlining the potential risks raised by these services if they were left unregulated and by identifying potential requirements for those service providers.

In our view, investment services on crypto-assets should be subject to the following prudential requirements:

- Receipt and transmission of orders on digital assets on behalf of third parties;
- Digital assets portfolio management services on behalf of third parties;
- Investment advice to digital assets holders;
- Underwriting of digital assets;
- Guaranteed investment of digital assets;
- Non-guaranteed investment of digital assets.

Crypto-assets are not banknotes, coins or scriptural money. For this reason, crypto-assets do not fall within the definition of ‘funds’ set out in the Payment Services Directive (PSD2)36, unless they qualify as electronic money. As a consequence, if a firm proposes a payment service related to a crypto-asset (that do not qualify as e-money), it would fall outside the scope of PSD2.

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

- Yes
- No
- Partially
- Don’t know/no opinion

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

As a preliminary remark, the activity of receiving funds (legal tender) on behalf of a buyer, no matter the underlying asset sold, and then transferring those funds to the seller would already qualify as a ‘payment service’ under PSD2. This particular activity and all activities qualified as the provision of ‘payment services’ linked to crypto-asset exchanges are therefore already subject to all PSD2 rules.

We also understand that this question is relevant only to crypto-assets that were defined as ‘payment tokens’ (and ‘stablecoins’). As we underline in the next paragraphs we will prefer the term...
‘exchange token’ instead of ‘payment token’ as the latter might create confusion between ‘payment services’ and the activity outlined in the question.

Pursuant Article 4 (5) PSD2, a ‘payment transaction’ means “an act […] of placing, transferring or withdrawing funds” where ‘funds’ are defined as “banknotes and coins, scriptural money or electronic money” under Article 4 (25) PSD2. Subsequently, the activity described in the question does not qualify as an execution of a payment transaction since crypto-assets are not legal tenders within the European Economic Area (EEA) or elsewhere. Furthermore, although some market participant perceive them as a ‘mean of payment’, crypto-assets do not respond to its legal definition either, as no central bank or public authority backs their value. Therefore, from a legal perspective, the exchange of crypto-assets does not currently qualify as a ‘payment transaction’ and crypto-assets themselves do not qualify as a ‘mean of payment’.

Notwithstanding this background, we acknowledge that some market participants currently use crypto-assets as a ‘mean of exchange’. For this particular reason, we strongly prefer the term ‘exchange token’ to ‘payment token’.

Furthermore, in our view, those tokens are digital assets in the sense of article L. 54-10-2 2° of the Monetary and code. Therefore, it remains unclear whether the PSD2 rules apply. In any case, we should rather adopt a risk-based approach.

The conservation of those digital assets by a third party and the execution of the ‘exchange token’ transactions may indeed bear significant risk among which we may stress cyber-security and operational risks, consumer protection risk, and, above all, money laundering and terrorist financing risk. Therefore, from a policy standpoint, to promote a sound and innovative ecosystem, the activity of making exchange transactions with crypto-assets should be subject to rules proportionate to the risk faced by the those service providers.

As a first step, an EU-level definition of ‘exchange token transactions’ and ‘exchange tokens’ is required. A broad definition of what those tokens are can already be found under French national law since 2019:

- “any digital representation of a value that is not issued or guaranteed by a central bank or a public authority, where it is not necessarily attached to a legal tender and where it does not hold the legal status of money, but is accepted by natural or legal persons as a mean of exchange and that may be transferred, stored or electronically exchanged” (Article L54-10-1 of the Code monétaire et financier).

France’s national framework, under PACTE Law, also grasps the prudential risks behind the activity described in the question. Entities that offer to buy and sell crypto-assets and/or that hold ‘exchange token’ (and other types of crypto-assets) on behalf of others for either securely storing the token or transferring it (that is executing ‘token exchange transaction’) are registered and supervised. Under this regulatory framework, they are subject to governance rules (notably fit & proper rules on the management body), anti-money laundering rules, and own funds requirement that are proportionate to the risk they bear.

It is also our view that where the crypto-asset service provider provides ‘payment services’ as defined under PSD2, it should be subject to both the requirements of PSD2 and of the new regulatory framework applicable to crypto-asset services. As such, rules applicable to protection of users’ funds, such as refund in case of unauthorised or defective transaction, liability shift between parties involved in the transaction, transparency requirements, should apply. Rules applicable to supervision and execution of the payment transaction should be adapted to the features of crypto payment transaction.

Finally, while an EU-level regulation is most welcome, we should adopt a risk-based approach to promote those innovative services while preserving a secure payment environment.

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.

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

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price manipulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Volume manipulation (wash trades…)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Pump and dump schemes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Manipulation on basis of quoting and cancellations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Dissemination of misleading information by the crypto-asset issuer or any other market participants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Insider dealings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

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.

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

The holding of cryptocurrencies is generally highly concentrated. The example of the Bitcoin, the most traded cryptocurrency, gives a clear evidence: almost 3% of the ip addresses owns 95% of the bitcoins market and 0.06% of the ip addresses owns 62% of the bitcoins market (figure 1). This level of market concentration might facilitate price manipulation and volume manipulation. In fact, there is evidence of wash trade, an analysis published by Bitwise shows that 95% of bitcoin spot trading is faked by unregulated exchanges. Only $273 min of average daily bitcoin volume (about $6 billion) would be effective transactions.

*Figure 1: High level of market concentration*
The level of concentration of the bitcoin market is stable over time. This eases the price and volume manipulations, which we consider as the highest market integrity risk. Crypto-assets have higher volatility than other assets (figure 2), in case of price manipulation contracting parties might face important losses.

**Figure 2 : Crypto-assets 90d volatility higher than other assets**

Additionally, market manipulation can come from manipulation of order books when platforms have such order books. Indeed, it is relatively easy to manipulate prices through techniques which are the same as for financial instruments traded on exchanges. Manipulation may occur principally through setting the price at an abnormal or artificial level when buying or selling or by giving false or misleading indications on offer, demand or prices.

Insider dealing may also occur. Risks are probably here a little less important than for classical financial instruments like shares, where inside information relates directly to a company which can produce a lot of them related to the normal course of its activity.

As far as crypto assets are concerned, the underlying object is less able to produce inside information.
when the cases of crypto assets is a payment token like bitcoin. However it is much more able to produce one when a crypto asset is an investment token or a utility token.

Inside information is also to arise when it relates to orders which are going to be introduced in the order book, like for classical financial instruments.

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.

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

We agree that market integrity on crypto-assets needs to be ensured. We have two options regarding the regulation of the crypto-assets market:

1. The regulation is performed by an independent agency. This option offers the capacity to i) guarantee an independence from national authorities/government and the industry, ii) allow the industry to maintain its capacity for innovation and to use the latest production techniques, iii) contribute to a better coordination at European level and reinforce the prominence of a single policy through European Union. On the other hand, the size of the crypto-asset sector might be too small for having a dedicated national agency and it might conduct to decrease the national independency.

2. The regulation is performed by the national authority. This option guarantees the capacity for the national authority to monitor and regulate the crypto-asset activity.

If we favour option 2, there should be a coordination at European level in order to ensure a level playing field between member states.

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

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

- Yes
- No
- Don’t know/no opinion

Please explain your reasoning (if needed). If yes, please explain how you would see this best achieved in practice.

The identification of the parties to transactions seems essential in order to i) optimize the efficiency of the crypto-asset market and to ii) ensure that transactions are compliant with money laundering and terrorist financing and any other existing or future regulation related to such market.

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?

We might envisage to use the experience of the European directive 2015/849 regarding the use of
2. Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT)

Under the current EU anti-money laundering and countering the financing of terrorism (AML/CFT) legal framework\(^37\), providers of services (wallet providers and crypto-to-fiat exchanges) related to ‘virtual currency’ are ‘obliged entities’. A virtual currency is defined as: “a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically”. The Financial Action Task Force (FATF) uses a broader term ‘virtual asset’ and defines it as: “a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations\(^38\). Therefore, there may be a need to align the definition used in the EU AML/CFT framework with the FATF recommendation or with a ‘crypto-asset’ definition, especially if a crypto-asset framework was needed.

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

- Yes
- No
- Don’t know/no opinion

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

The definition of ‘virtual currency’ provided by the 5th AML/CFT Directive (“5AMLD”) is more restricted than the FATF definition. Extending the existing ‘virtual currency’ definition in the EU AML/CFT legal framework in order to align it with a broader definition such as the FATF’s definition would be an appropriate regulatory response to the diversification of crypto-assets. Indeed, the 5AMLD refers to ‘virtual currency’ only as a means of payment. Yet, crypto-assets are not used as means of payment only but also for investment purposes. Under a bespoke EU regime for crypto-assets, crypto-assets could be defined as tokens or as ‘a digital representation of value’ which may be used as ‘a means of exchange or transferred, stored or electronically exchanged’. In our opinion, this definition better encompasses crypto-assets multiple purposes as a payment means, a store of value and as an investment asset. Consequently, we favor a wider definition of crypto-assets such as the FATF’s definition, which presents these digital assets as ‘a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes’. In our view, this definition is better tailored to the variety of existing crypto-assets as it encompasses all characteristics of crypto-assets’ purposes. It’s also important to emphasize that if the definition of ‘virtual currency’ was aligned with the FATF’s definition, it could imply that central bank digital currencies (CBDC) could be qualified as ‘virtual currency’ unless they are already qualified as e-money.

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

42) Beyond fiat-to-crypto exchanges and wallet providers that are currently covered by the EU AML/CFT framework, are there crypto-asset services that should also be added to the EU AML/CFT legal framework obligations? If any, please describe the possible risks to tackle.

The FATF has a broader approach in its recommendations than the current scope of the EU AML regulation. Indeed, the standards also cover crypto-to-crypto exchanges, providers that conduct transfer of crypto-asset and providers that participate in and provide financial services related to an issuer’s offer and/or sale of a virtual asset. French authorities are of the opinion that the EU scope should be extended to these entities, with a special focus on crypto-to-crypto exchanges. Indeed, Crypto-to-crypto exchanges represent high ML-TF risk since they allow exchanges between crypto-assets based on traceable blockchains and crypto-assets based on untraceable blockchains that allow anonymity of transactions (anonymity-enhanced cryptocurrencies, AEC). A common EU approach is also necessary because some countries have already decided to broaden the scope of the obliged entities, after the FATF have finalised its standards last year. However, extending the scope of obliged entities and of the requirements applied to these entities (travel rule in particular) raises major questions which are detailed below and that would have to be dealt with at the EU level.

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

---

38 FATF Recommendations
Please explain your reasoning (if needed).

Harmonizing the EU AML-CFT standards with those of the FATF seems consistent with the EU willingness to increase its leadership within this organization. Besides, it is necessary to ensure a maximum harmonization, EU wide, of both the scope of obliged entities and their regulatory/authorization regimes in order to avoid any regulatory competition between the member states.

As a result, it seems necessary to align the scope of obliged entities under the EU AML/CFT framework with FATF Recommendation 15 in order to avoid any discrepancy.

However, a dedicated work on the definitions of the obliged entities should be done, to clarify the activities covered by the standards (what services are covered by the “participation in and provision of financial services related to an issuer’s offer and sale of virtual assets”).

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

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.”

The FATF Standards do not apply to peer-to-peer transactions i.e. transactions conducted without the use of a VASP, between users via unhosted wallets. In absence of any customer due diligence (CDD) obligations, peer-to-peer transactions represent enhanced ML-TF risks. However, only intermediaries that are obliged entities are required to implement AML/CFT measures but individuals acting on their own behalf should not.

Many suggestions have been made during FATF PDG sessions for inciting individuals to be clients of VASPs, such as mandating that users undergo Diligence prior to gaining access to the crypto-asset system, making the use of a regulated VASP mandatory on at least one side of every transaction or mandating that users only hold crypto-assets in a hosted wallet which they would have to undergo CDD to access.

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

- Yes
- No
- Don’t know/no opinion

Please explain your reasoning (if needed).

Recommendation 16 provides that VA transfers implying at least one VASP must contain information concerning ordering and beneficiary parties. VASPs and VA transfers fall outside the scope of regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC)
No 1781/2006 that transposes Recommendation 16 requirements in the EU legal framework. Recommendation 16 requirements should be introduced in the EU AML/CFT legal framework to ensure level playing field between VASPs registered in all EU countries and to enhance the effectiveness of freezing-asset measures, as crypto-assets transfers are inherently considered as cross-borders by FATF. Furthermore there are still many difficulties concerning transparency of virtual assets transfers (see FATF guidance for a risk-based approach “Virtual assets and virtual asset service providers” of June 2019). Additional details should be provided concerning practical implementation of these requirements since it’s a technological challenge.

46) In your view, do you consider relevant that the following requirements are imposed as conditions for the registration and licensing of providers of services related to crypto-assets included in section III. B? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

<table>
<thead>
<tr>
<th>Requirement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Please explain your reasoning (if needed).

As an introduction, the financial crisis exposed that the weakness in corporate governance have contributed to excessive and imprudent risk-taking by directors and senior management. The assessment of fit and proper is key for the financial system. This assessment promotes good reputation of the financial system and increase trust on it. As a result, we consider that the fit and proper shall not limit to the money laundering. Thus, internal governance is fundamental to permit to the institutions and the banking system to operate well. A good internal governance builds confidence in the reliability of the financial system and contribute to the economy as a whole. In this context, we analyse the ability of service provider to demonstrate they have all the controls in place in order to be able to comply with their obligations under the anti-money laundering framework, and internal governance, as highly relevant. To summarize, would the mentioned providers of services related to crypto-assets included in section III.B be subject to regulatory framework including for AML/CFT and internal control purposes, then fit & proper tests (which shall be extended to significant shareholders) and AML/CFT internal controls would be compulsory.

39 FATF Recommendations
3. Consumer/investor protection

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. 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, others 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.

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information provided by the issuer of crypto-assets (the so-called ‘white papers’)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Limits on the investable amounts in crypto-assets by EU consumers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Suitability checks by the crypto-asset service providers (including exchanges, wallet providers…)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Warnings on the risks by the crypto-asset service providers (including exchanges, platforms, custodial wallet providers…)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Given the informational gap between crypto-asset service providers and their clients and the high risk of capital loss associated to these assets, we consider that all crypto-asset service providers should be required to abide by comprehensive consumer protection measures. Consequently, they should provide their clients with clear, exact and non-misleading information and advertisements. They should be required to alert their clients on the risk of capital loss entailed by investment in crypto-assets. They should make their fees and commissions policy public. They should set up efficient processes to answer their clients’ claims swiftly.

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?
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.

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

Please explain your reasoning (if needed).

We do not believe that the standards of consumer/investor protection applied to crypto-assets should vary depending on the crypto-assets nature or function. All crypto-assets should be subject to the same consumer/investor protection rules as all investment entail the same risk, namely a risk of capital loss.

However, it is very important to clearly distinguish between crypto-assets and security tokens, from a consumer/investor protection point of view, as in French national law, security tokens are financial instruments and as such falls within the scope of financial instruments regulation and without the scope of consumer/investor protection. In short, all security tokens qualifying as “transferable securities” within the meaning of the MiFID directive should be governed by the prospectus (PD3) legal regime. A legal clarification, through a Q&A published by the EU Commission or ESMA, should provide some specific and practical guidance with respect to the applicability of “transferable securities” to security tokens. As for the other tokens, the same consumer/investor protection should apply whatever their prevalent economic (i.e. payment tokens, stablecoins, utility tokens…) or social function.

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’).

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

What matters most is that when crypto-assets are bought via an initial coin offering token issuers be required to publish a whitepaper. This document should contain useful information to the public on the token and on its issuer.

Please explain your reasoning (if needed).

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

- Yes
- No
- Don’t know/no opinion

Please explain your reasoning (if needed).

European legislation could make no distinction between crypto-assets obtained against payment and those obtained for free if it were to protect consumers effectively. Indeed, crypto-assets obtained for free may lead consumers to buy additional crypto-assets.

The vast majority of crypto-assets that are accessible to EU consumers and investors are currently issued outside the EU\(^43\). If an EU framework on the issuance and services related to crypto-assets is needed, the question arises on how those crypto-assets issued outside the EU should be treated in regulatory terms.

51) **In your opinion, how should the crypto-assets issued in third countries and that would not comply with EU requirements be treated? Please rate each proposal from 1 to 5, 1 standing for "not relevant factor" and 5 for "very relevant factor".**

<table>
<thead>
<tr>
<th>Proposal</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Those crypto-assets should be banned</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Those crypto-assets should be still accessible to EU consumers/investors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^{42}\) See Autorité des Marchés Financiers, French ICOs – A New Method of financing, November 2018

\(^{43}\) In 2018, for instance, only 10% of the crypto-assets were issued in the EU (mainly, UK, Estonia and Lithuania) – Source: Satis Research.

Please explain your reasoning (if needed).

The commercialization, distribution and sale of third country crypto-assets not abiding by the future European framework should be banned. Should the future European framework on crypto-assets take the form of a regulation, it should ban those third country (or even European) crypto-assets that pose a threat to investor protection and the integrity or to the orderly functioning of financial markets.

This ability to ban should de facto be the corollary of the set-up, at European level, of a regulatory regime based on mandatory requirements to be met by crypto-assets, and notably stablecoins, in particular those reaching a global footprint, so that those assets issued in third countries and that would not comply with those requirements, would be banned.

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 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.

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

The French national law and the NCA’s set of procedures provide a sound regulatory and supervisory framework to ensure both an effective licensing and supervisory process for the crypto-asset service providers operating in our jurisdiction (including digital asset issuance, trading platforms, exchanges, provision of custodial wallet services and other service providers, in particular when they provide cross-border services), while maintaining a certain level of flexibility for innovation to grow. A more mature experience in the market with new initiatives such global stablecoins might be required in order to assess the need to prescribe supervisory coordination or supervision at EU level.

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

Assuming an effective supervisory process at national level supported by the national regulatory and supervisory frameworks (see answer to previous question), tools to be used at national level for supervising digital asset service providers would be also relevant at EU level. Fintech innovation hubs provided by NCAs at French level (such as ACPR Fintech Innovation hub), supplemented by the national Forum Fintech and the related workstreams (with representatives from both NCAs and the financial industry) offer an efficient way to assess the underlying technologies, either current or emerging ones. Moreover, the SupTech initiative and the asserted openness to experimentation, supported both by ACPR, are prone to fulfill this objective. Such national frameworks, openness and initiatives would aim to tackle new issues that might arise in the crypto-asset sector, which is
characterized by innovative services, processes and underlying technologies, including new market initiatives like *global stablecoins*. Such mechanisms exist also at EU level and might also serve the same objectives: see for example the ESAs’ SupTech strategies and the EFIF joint committee (European Forum for Innovation Facilitators).

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 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) on trading, post-trading and other financial services concerning security tokens, such as asset management, the purpose of this part of the consultation is to seek stakeholders’ views on the issues identified below that are relevant for the application of the existing regulatory framework to security tokens.

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

Current trends concerning security tokens

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

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

---

45 Trading venues are a regulated market, a multilateral trading facility or an organised trading facility
46 European Markets Infrastructure Regulation (648/2012/EU)
48 At level 1, the European Parliament and Council adopt the basic laws proposed by the Commission, in the traditional co-decision procedure. At level 2 the Commission can adopt, adapt and update technical implementing measures with the help of consultative bodies composed mainly of EU countries representatives. Where the level 2 measures require the expertise of supervisory experts, it can be determined in the basic act that these measures are delegated or implemented acts based on draft technical standards developed by the European supervisory authorities.
49 For example the German Fundament STO which received the authorisation from Bafin in July 2019
50 See section IV.2.5 for further information
platforms. 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 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 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.

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)?

Regarding STOs, several offerings based on security tokens have already been carried out in Europe (France, Germany, and United Kingdom) and the United States, and several other issuance projects are underway.

Regarding the secondary market of security tokens, very few security token trading platforms are to date operational, but there are numerous plans, including among large institutional players. In the meantime, new so-called “tokenization” platforms have appeared, with a view to assisting market participants in the “tokenization” of financial instruments.

A growing interest is being shown for the phenomenon of Security Token Offerings (STOs).
Among these projects, the FORGE project that issued security tokens for an amount of €100m finalised on 18 April 2019 concerning housing financing bonds (refinancing vehicle for group housing mortgage loans), subscribed entirely within the group Société Générale. It cannot be classified as a public offer and is not covered by the Prospectus Regulation. A second issuance of tokens is planned. Another example of company that has launched an STO could be given with the Carthagea’s STO made in March 2019 concerning shares designed to finance nursing homes for the elderly in Tunisia. It is made by a French project promoter to French investors subscribing for at least €100,000. Under current law it is therefore not considered as a public offer and is not covered by a prospectus.

Further, several security tokens have been presented to the Fintech, Innovation and Competitiveness department of the AMF.

51 Type of crypto-asset trading platforms that holds crypto-assets on behalf of its clients. The trade settlement usually takes place in the books of the platforms, i.e. off-chain.
52 In the trading context, going peer-to-peer means having participants buy and sell assets directly with each other, rather than working through an intermediary or third party service.
53 Type of crypto-asset trading platforms that do not hold crypto-assets on behalf of its clients. The trade settlement usually takes place on the DLT itself, i.e. on-chain.
55) Do you think that DLT could be used to introduce efficiencies or other benefits in the trading, post-trade or asset management areas?

<table>
<thead>
<tr>
<th>Option</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely agree</td>
<td>X</td>
</tr>
<tr>
<td>Rather agree</td>
<td></td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Rather disagree</td>
<td></td>
</tr>
<tr>
<td>Completely disagree</td>
<td></td>
</tr>
<tr>
<td>Don’t know / No opinion</td>
<td></td>
</tr>
</tbody>
</table>

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

Although there are still challenges to be addressed, we believe that DLT could bring a number of benefits to securities markets, especially (1) more efficient post-trade processes, (2) enhanced supervisory functions (3) greater security and resilience to cyber-attacks. Even though this goes beyond the scope of the question, it is worth noting however that DLTs may also give rise to new types of risks that would deserve to be properly addressed.

(1) More efficient post-trade processes due to the benefits of standardization

DLT could accelerate the clearing and settlement of certain securities transactions. The key benefits of DLT applied to post-trade processes is the reduction in costs for clearing, settlement, custody, registrar/notary services as well as compliance and risk monitoring. According to feedback from players who have used a blockchain to carry out an operation instead of traditional circuits, blockchain makes it possible to significantly streamline booking/post-trade processes (reduction of 40 to 60% of transaction steps) and reduce costs (A DVP operation using DLT accounts for 0.07 euro versus 0.25 euros for its equivalent on Target 2 Securities infrastructure).

These profits were noted at the end of an operation where only the securities leg had been tokenized, the profits to be expected if the cash leg would also be possible on chain would be even more significant.

According to the market players, the value of the DLT is high and sits in the standardisation of product (e.g. the possibility offered by smart contract to embark the complexity of the payoffs) as well as in the ability to better integrate market on a common and trustable technology. The secondary market details can be easily read by anyone on the blockchain (including transaction cost).

- Facilitate the safekeeping and the record-keeping of ownership

It may also facilitate the safekeeping and the record-keeping of ownership of certain assets by providing a single market participants shared ‘record’ that enhance the traceability of transactions and make ultimate ownership transparent throughout the security life cycle. Therefore, these enhancements would be particularly useful for those assets for which post-trade processes are very cumbersome and costly today.

For instance: The use of self-executing computer protocol translating contractual terms into computational material (“smart’ contracts”) could enhance the enforcement the automation of back office processes, reduce errors as well as legal disputes.
- **A real-time settlement**
  Clearing and settlement processes could become almost instantaneous with DLT. Indeed, trade confirmation/affirmation, allocation and settlement could be combined into a single step (e.g. moving from the current T+2 standard to almost instantaneous settlement using DLT). Thus, this could de facto reduce counterparty risk and as well as settlement failures.

- **Reduced counterparty credit risk**
  DLT may lead to shorter settlement cycles that should reduce counterparty credit risk for trades and thus facilitate reconciliations and collateral processes. Since the risk of exposure to the "transaction settlement time span" could be reduced, it could thus mitigate the central clearing and collateral posting counterparty risk of clearing houses.

(2) **Enhanced supervisory functions with a direct access for regulators**
  A DLT record application could enhance supervision functions of regulators, by facilitating the collection, consolidation and sharing of data in real time from firms to regulators. For example: Regulators could be granted special access rights on a DLT infrastructure in order to consult or use details on transactions stored on the DLT.

(3) **Greater security and resilience to a cyber-attacks**
  The distributed nature of DLT could facilitate access to data and data protection in case of a cyber-attack.

  - **Data protection**
    DLT generally use strong and sophisticated encrypted solutions which provide an additional layer of data protection stored on DLT compared to existing systems. In this respect, decentralised DLT infrastructures could also reduce "Single Point Of Failure" risk present in more centralised architecture.

  - **Access and recovery of data**
    Since each market participant represents a node on the DLT infrastructure, the simultaneously corruption of all nodes on such distributed infrastructure become more difficult. This also could reduce the need for costly recovery plans

In addition, it is worth noting that although permissioned DLTs could be easier to conceive/design when it comes to securities markets governance, some of the benefits attached to permissionless DLTs among which the security could be lost or significantly reduced in a permissioned framework.

---

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?**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely agree</td>
<td></td>
</tr>
<tr>
<td>Rather agree</td>
<td></td>
</tr>
<tr>
<td>Neutral</td>
<td>X</td>
</tr>
<tr>
<td>Rather disagree</td>
<td></td>
</tr>
<tr>
<td>Completely disagree</td>
<td></td>
</tr>
<tr>
<td>Don't know / No opinion</td>
<td></td>
</tr>
</tbody>
</table>

**Please explain your reasoning (if needed).**

From a pure theoretical point of view, decentralised technology seems less risky than a single intermediary, which creates a potential single point of failure: risks in terms of bankruptcy or cyber attacks are de facto more limited in the context of a network of participants rather than with a
unique intermediary.

Nevertheless, the use of DLT potentially creates new risks or exacerbates existing ones (e.g. risk of an "irretrievable" code error; risk to the sovereignty of the financial system by a 51% attack from another geographical area; cyber risks of a different nature etc.). Additionally, there is no reliable means of settlement at this stage.

It seems premature to fully appreciate the nature and level of those risks, the changes that the technology could have on the financial stability and therefore regulatory response that may be needed, given that the technology is still evolving and practical applications are limited both in number and scope.

Before drawing conclusions about possible systemic risks related to blockchain, the technology should be tested in order to assess its advantages and disadvantages. Therefore, there is an interest in having the possibility to make use of a transition period involving the creation of a "digital lab" at the EU level for DLT projects in the financial sector (security tokens).

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.

Although DLT were first developed in the realm of virtual currencies, they have emerged since 2015 as an innovation that may change the current paradigm of financial markets, particularly as far as market infrastructures and post-markets are concerned. Distributed ledger technologies (DLTs) allow different users to share the management of data, possibly to process financial market transactions and keep track of their holdings of assets (securities, coins, etc.) and cash.

Applications for DLT in capital markets are multiplying fast and moving rapidly towards implementation. DLT has not only the potential to reduce costs and risks in the investment industry: In time it could re-order existing value chains, ushering in profound changes to capital market processes and structures. DLT represents a varied, adaptive group of consensus-based technologies with unique features and benefits and it is ideally suited to performing a range of capital markets functions.

Practical uses are multiplying, the post-trade space presents great opportunities of applications and it would facilitate trading. DLT can establish a 'single version of truth' and allows it to cut across corporate boundaries and existing market structures. One of the most obvious applications for DLT is as a single asset register for an asset manager or broker-dealer. Such technology would eliminate internal reconciliations, enhance capital efficiency and give clients or regulators controlled access to real-time data. Extending this logic across multiple market participants opens up vast potential benefits in the post-trade arena.

Mutually-operated ledgers could transform clearing, settlement and reporting for OTC securities and derivatives markets. Such a ledger would release huge amounts of capital by reducing settlement periods and giving users a single view of the location and eligibility of collateral assets.

In theory, tokenisation – using tokens to represent legal title or right related to financial assets – could enable DLT to act as a trading venue, not just a settlement venue.

Some compelling applications for DLT in the capital markets include:

i. Payments. DLT can streamline end-to-end value transfers, reducing costs, operational risks and settlement periods;
ii. Back office in Bank finance: syndicating lending, trade finance and other forms of bank finance still rely on paper documents and manual processes. DLT could
transform this by providing a shared record of shipments, ownership, financing and insurance:

iii. Fund administration: A distributed ledger recording the creation, redemption and transfer of fund units would eliminate many of the current complexities of fund administration. It could unify cross-border sales, processing and transfer;

iv. Customer identification (if DLT would not qualify as “systems”). An industry-wide distributed ledger could host a shared record of beneficial owners. Such a utility would give appropriate, permissioned access to market participants allowing immediate KYC and AML checks, assisting with client on-boarding and enhancing tax reporting.

However in order to achieve these theoretical benefits, DLT technology has to prove its ability to create the same positive externalities as existing technologies / infrastructures. In particular, operational resilience / performance and effective volumes may pose a challenge. Moreover, several legal aspects have to be addressed adequately to ensure a high level of security for the financial system (settlement finality in particular, please refer to answer to questions 93 to 96).

It shall also be stressed that the emergence of numerous DLT systems may create technological fragmentation across payments / securities markets, which would be prejudicial to Capital Markets Union.

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?

<table>
<thead>
<tr>
<th>Completely agree</th>
<th>Neutral</th>
<th>Rather disagree</th>
<th>Completely disagree</th>
<th>Don't know / No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please explain your reasoning (if needed).

Banque de France broadly agrees that a gradual regulatory approach in the area of post-trading would be appropriate, under the condition that it preserves necessary legal and operational safeguards. Only permissioned centralized solutions can indeed be considered as suitable at this stage.

In France, the recent implemented “PACTE” law is the new legal framework dedicated to tokens (ICO, STO, etc.). The new law introduces on optional “regime” as a gradual regulatory approach to take into consideration the new economic and technological environment.

The development of the “crypto” environment will be facilitated by an innovative regulation taking into account the specificities of the new business models and by providing the players with needed legal protection to further develop their activities. Legal clarification will be necessary to allow for a common and shared understanding of the qualification of security tokens; however any proposed legal clarification should be carefully assessed in order to comprehensively identify possible consequences (legal and operational risks, among others from a settlement finality perspective; possible post-market fragmentation; competition
issues…).

Banque de France insists on the need to continue favouring a settlement in central bank money, to avoid both (i) the reintroduction of credit and liquidity risk in post-trading and (ii) operational reliability issues that would jeopardize delivery versus payment and re-introduce principal risk.

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

1.1. Financial instruments

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

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

In its Advice, ESMA 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.

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?

54 MiFID Directive (2014/65/EU)  
55 MiFIR Regulation (600/2014/EU)  
Please explain your reasoning (if needed). [Insert text box]

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harmonise the definition of certain types of financial instruments in the EU</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide a definition of a security token at EU level</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

61) How should financial regulators deal with hybrid cases where tokens display investment-type features combined with other features (utility-type or payment-type characteristics)? Please rate each proposal from 1 to 5, 1 standing for “not relevant factor” and 5 for “very relevant factor”.

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

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

1.2. Investment firms

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

<table>
<thead>
<tr>
<th>Choice</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely agree</td>
<td></td>
</tr>
<tr>
<td>Rather agree</td>
<td>X</td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Rather disagree</td>
<td></td>
</tr>
<tr>
<td>Completely disagree</td>
<td></td>
</tr>
<tr>
<td>Don’t know / No opinion</td>
<td></td>
</tr>
</tbody>
</table>

Please explain your reasoning (if needed).

We think that existing rules and requirements for investment firms may be applied in a DLT environment for security tokens. For non-security tokens, it may raise issues to apply existing rules and requirements for investment firms in a DLT environment.

We also would like to mention that with the introduction of the IFD directive, two distinct regulations would potentially apply (CRD and IFRD), considering the size of consolidated assets.

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

<table>
<thead>
<tr>
<th>Choice</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely appropriate</td>
<td></td>
</tr>
<tr>
<td>Rather appropriate</td>
<td>X</td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Rather appropriate</td>
<td></td>
</tr>
<tr>
<td>Completely inappropriate</td>
<td></td>
</tr>
<tr>
<td>Don’t know / No opinion</td>
<td></td>
</tr>
</tbody>
</table>

Please explain your reasoning (if needed).

A clarification or a guidance on applicability of such rules and requirements would be “rather appropriate” at EU level for “level playing field” concerns, however the technology is still evolving and the regulations throughout the EU member states are not yet harmonized.

1.3. Investment services and activities

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

64) Do you think that the current scope of investment services and activities under MiFID II is appropriate for security tokens?
The current scope of investment services and activities under MIFID II is “completely appropriate” for security tokens. Under French law, security tokens qualified as “securities” and the legal regime provided by MIFID II is fully applicable to security tokens because it is deemed completely appropriate.
65) Do you consider that the transposition of MiFID II into national laws or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT for investment services and activities? Please explain your reasoning (if needed).

Please explain your reasoning (if needed).

We do not consider that the transposition of MiFID II into national laws or existing market practice in France would facilitate or otherwise prevent the use of DLT for investment services and activities. French regulations are neutral.

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.

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

The existing regulatory framework might not be enough to address the specific case of instruments using DLT.

In particular, concerning platforms, there might be a lack of clarity on how the existing rules apply to so-called decentralised and hybrid models that use smart contracts to match orders and/or to conclude transactions.

1.5. Investor protection

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

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

---

58 Recital 8 of MiFIR.
Would you see any merit in establishing specific requirements on the marketing of security tokens via social media or online? Please explain your reasoning (if needed). [Insert text box]

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

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.

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

DLT has the potential to make the financial sector more efficient.

It may substantially change the way financial markets are operating today, promising important cost savings and efficiency gains in particular in the post-trade space.

In this way, SME may benefit from some such cost savings to access more easily to financial markets, including SME Growth Markets.

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 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.

Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed? Please explain your reasoning (if needed).
As defined by article 4(1)(41) and in accordance with Art 48(7) of MiFID by which trading venues should only grant permission to members or participants to provide direct electronic access if they are investment firms authorised under MiFID or credit institutions authorised under the Credit Requirements Directive (2013/36/EU)
1.8. Admission of financial instruments to trading

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

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

1.9. Access to a trading venues

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

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

The main benefits of allowing direct access to clients (including retail investors) are cost savings with significant reductions of fees.

However, current use of intermediaries, such as regulated investment firms and credit institutions, grants protection for investors. They have the resources to comply with the financial market requirements (margins and deposit, IT infrastructure, competences and Ressources, etc.). Investors, especially retail ones, may lack these resources to cope with these requirements.

Lack of robustness of single investors may also strengthen the risks faced by financial infrastructures, such as trading venues or CCP.

A direct access to trading venues to a broader base of clients should then be granted with caution. It should be limited to simple financial instruments (plain vanilla products).
1.10. **Pre and post-transparency requirements**

MiFIR\(^6^0\) 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\(^6^1\) 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

---

\(^6^0\) In its Articles 3 to 11

\(^6^1\) 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.
circumstances, it seems difficult to clearly determine the need for any possible adaptations of existing rules due to the lack of actual trading of security tokens.

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

<table>
<thead>
<tr>
<th>Opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely agree</td>
</tr>
<tr>
<td>Rather agree</td>
</tr>
<tr>
<td>Neutral</td>
</tr>
<tr>
<td>Rather disagree</td>
</tr>
<tr>
<td>Completely disagree</td>
</tr>
</tbody>
</table>
| Don't know / No opinion      | X

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

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

11.1. Transaction reporting and obligations to maintain records

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

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

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.

\(^2\) In its Article 25 and 26

Security tokens are covered by the MAR framework where they fall within the scope of that
regulation, as determined by its Article 2. Broadly speaking, this means that all transactions in security tokens admitted to trading or traded on a trading venue are captured by its provisions, regardless of whether transactions or orders in those tokens take place on a trading venue or are conducted over-the-counter (OTC).

2.1. Insider dealing

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

77) Do you think that the current scope of Article 8 of MAR on insider dealing is appropriate to cover all cases of insider dealing for security tokens? ACPR-

Under French law, committing an insider dealing is punished by 5 years of imprisonment and a 100 millions euros fine. This insider dealing may be committed by any natural or legal person who holds a privileged information because of its occupation or its functions (article L.465-1 of the French monetary and financial code [French MFC]. This article is similar to the dispositions of article 8.4 of the Market Abuse Regulation (MAR).

In our opinion, the afore-mentioned dispositions on insider dealing could be extended to apply to any legal or natural person in the crypto-asset ecosystem who holds information on the future launching of an initial coin offering.

2.2. Market manipulation

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

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

78) Do you think that the notion of market manipulation as defined in Article 12 of MAR is sufficiently wide to cover instances of market manipulation of security tokens?

Under French law, market manipulation is punished by criminal sanctions. Article L.465-3-1 of the French monetary and financial code (French MFC) defines market manipulation as two
types of conduct:
- Entering into a transaction, placing an order to trade or any other behavior which is susceptible to give false information on the offer, the demand or the price of a financial instrument; or
- Entering into a transaction, placing an order to trade or any other behavior, which is likely to set the price of a financial security at an unusual or artificial level.

The French definition of market manipulation is thus rather close to the definition of market manipulation as the one enshrined in article 12.1 of the Market Abuse Regulation (MAR).

In our view, it could be assumed that initial coin offerings of tokens enter into the scope of both French MFC and MAR’s dispositions on market manipulation since it is possible for a crypto-asset issuer or service provider to have access to more information on tokens than the larger public of investors. If they were to act upon their privileged information, they could manipulate tokens’ prices accordingly.

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?

We believe that manipulative trading on stable coins could affect the price or value of their underlying assets, which could be financial instruments covered by the Market Abuse Regulation.

3. Short Selling Regulation (SSR)

The Short Selling Regulation\(^{64}\) (SSR) sets down rules that aim to achieve the following objectives: (i) increase transparency of significant net short positions held by investors; (ii)

\[^{63}\text{Under MiFID Article 4(1)(24) ‘trading venue’ means a regulated market (RM), a Multilateral Trading Facility (MTF) or an Organised Trading Facility (OTF’)}\]

\[^{64}\text{Short Selling Regulation (236/2012/EU)}\]
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\textsuperscript{65}, security tokens fall in the scope of the SSR where a position in the security token would confer a financial advantage in the event of a decrease in the price or value of a share or sovereign debt. However, ESMA remarks that the determination of net short positions for the application of the SSR is dependent on the list of financial instruments set out in Annex I of Commission Delegated Regulation (EU) 918/2012), which should therefore be revised to include those security tokens that might generate a net short position on a share or on a sovereign debt. According to ESMA, it is an open question whether a transaction in an unregulated crypto-asset could confer a financial advantage in the event of a decrease in the price or value of a share or sovereign debt, and consequently, whether the Short Selling Regulation should be amended in this respect.

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

<table>
<thead>
<tr>
<th>Transparency for significant net short positions</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions on uncovered short selling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Competent authorities’ power to apply temporary restrictions to short selling</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

In order to apply the Short Selling Regulation (SSR) to security tokens, these tokens would have to qualify as financial instruments under MiFID II (article 1.1 of SSR). This criterion might not be met by all security tokens depending on their respective characteristics. A diverging qualification of security tokens among different member states might lead in turn to a diverging application of SSR.

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

81) Have you ever detected any unregulated crypto-assets that could confer a financial advantage in the event of a decrease in the price or value of a share or sovereign debt? [Insert text box]

N/A

4. Prospectus Regulation (PR)

The Prospectus Regulation\textsuperscript{66} establishes a harmonised set of rules at EU level about the drawing up, structure and oversight of the prospectus, which is a legal document accompanying an offer of securities to the public and/or an admission to trading on a regulated market. The prospectus describes a company’s main line of business, its finances, its
shareholding structure and the securities that are being offered and/or admitted to trading

66 Prospectus Regulation (2017/1129/EU)
on a regulated market. It contains the information an investor needs before making a decision whether to invest in the company’s securities.

4.1. **Scope and exemptions**

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

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

<table>
<thead>
<tr>
<th>Completely agree</th>
<th>Rather agree</th>
<th>Neutral</th>
<th>Rather disagree</th>
<th>Completely disagree</th>
<th>Don't know / No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

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

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\(^67\) assist national competent authorities in their review of the
materiality and specificity of risk factors and of the presentation of risk factors across categories depending on their nature. The prospectus could include pertinent risks associated with the underlying technology (e.g. risks relating to technology, IT infrastructure, cyber security, etc…). ESMA’s guidelines on risk factors could be expanded to address the issue of materiality and specificity of risk factors relating to security tokens.

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

- Yes
- No
- Don’t know/no opinion

If yes, please indicate the most effective approach: a ‘building block approach’ (i.e. additional information about the issuer and/or security tokens to be added as a complement to existing schedules) or a ‘full prospectus approach’ (i.e. completely new prospectus schedules for security tokens). Please explain your reasoning (if needed). [Insert text box]

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

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

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

- Yes
- No
- Don’t know/no opinion

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

We see no rationale to have an ad hoc alleviated prospectus regime.

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

<table>
<thead>
<tr>
<th>Completely agree</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rather agree</td>
<td></td>
</tr>
<tr>
<td>Neutral</td>
<td></td>
</tr>
<tr>
<td>Rather disagree</td>
<td></td>
</tr>
</tbody>
</table>
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.

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

<table>
<thead>
<tr>
<th>Definition</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition of ‘central securities depository’ and whether platforms can</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>be authorised as a CSD operating a securities settlement system which is</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>designated under the SFD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition of ‘securities settlement system’ and whether a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

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

Don't know / No opinion X
Central Securities Depositories Regulation (909/2014/EU)
Please explain your reasoning.

As a starting point, Banque de France would like to stress the importance of central bank money settlement for transactions registered in permissioned networks and centralized platforms. The reasons that have historically and unanimously led to favor settlement in central bank money in recent decades (elimination of settlement risk inherent to the use of commercial banks as settlement agents) are also valid in this new technological environment. The notion of technological neutrality shall not lead to new vulnerabilities in this regard.

A reintroduction of credit and liquidity risk in securities settlement would be reinforced by operational issues, such as higher operational complexity when it comes to interfacing commercial banks’ systems and DLT environments, putting into question the reliability of delivery versus payment. This would, in turn, create principal risk among participants to the DLT permissioned networks and centralized platforms. Financial stability stakes may reappear, all the more since volumes could increase at sustained pace in the medium term. Furthermore, that would clearly lead to market fragmentation, which would be in full contradictions with the objectives of the CMU and with the recent progress in terms of European post-market integration.

Initiatives for technological experiences by central banks in terms of euro tokenization have recently been launched in order to test the possibility to settle security tokens against tokenized central bank money. To preserve the advantages of multiple issuers of settlement assets in providing innovative, efficient and safe means of payment, central banks as issuers of the reference settlement asset may contribute further in revisiting and improving the conditions under which they make available that settlement asset. Banque de France urges to wait for the results of these initiatives before taking premature and unwelcome decisions that would incentivize permissioned networks to recourse to commercial bank money.

Whether settlement of crypto-assets representing rights on underlying securities / financial instruments would fall under the definition of a ‘system’ under the SFD, and / or the definition of a CSD under the CSDR are fundamental and should be carefully assessed. Indeed answer to that question will have very significant consequences in terms of oversight / supervisory requirements and hence of the overall risks attached to DLT.

Banque de France’s stance (duly taking into account ESMA’s advice published in January 2019 on initial coin offering and crypto-assets) is that settlement of crypto-assets representing rights on underlying securities / financial instruments in permissioned networks and centralized platforms
should fall under the definition of a ‘system’ under the SFD for the following reasons:
- Settlement in DLT environment falls under the definition of a ‘transfer order’ as defined by
  the SFD (pending however a formal confirmation that tokenization is considered as a ‘book entry’
  and a kind of ‘dematerialization’, which in Banque de France’s opinion is the case despite the
  absence of definition of ‘book entry’ and ‘dematerialized form’)
- Settlement in DLT environment would necessarily entail common rules and standardized
  arrangements for the execution of transfer orders, between three or more participants
- Designation as ‘system’ under the SFD would bring the needed legal comfort on the
  transactions registered in DLT environments, as the discharging of obligations would undoubtedly
  qualify as ‘settlement’ (whether of cash of securities, or both)

However, the following aspects may hinder the designation as ‘systems’ by Members States:
- Governance of the system by the law of a Member State chosen by the participants, which
  may only be the law of a Member State in which at least one participant has its head office. It
  should be further investigated whether such a choice may be at odds with the jurisdiction in which
  the operator of the system is established, and may create conflicts of law.
- Legal clarification at EU level of the exact qualification of the various types of ‘crypto-assets’
  as ‘securities’, which may call for a revision of the SFD in order to explicitly encompass crypto-
  assets based on securities.

1. The definition of a CSD is given by the CSDR, which very closely intertwines with the definition
   of a securities settlement system and hence with the definition of a system under the SFD:
   - Only CSDs authorized under the CSDR can operate securities settlement systems (article
     16 of the CSDR);
   - Operating of a securities settlement system is a mandatory core service to be provided in
     order to be qualified and authorized as a CSD (article 2.1 of the CSDR).

Therefore, pending the legal clarification at EU level of the qualification of security tokens as
‘securities’, and depending on the scope of securities dealt with by a DLT permissioned network,
a CSDR authorization may be needed. This in turn raises the question of whether the constraints
set by the CSDR are proportional for permissioned DLT networks and may represent obstacles to
the effective development of innovative solutions for securities settlement.
Also depending upon the legal clarification at EU level of the qualification of security tokens as
‘securities’, the records on a DLT platform would be qualified as securities accounts and any
movement in the records of the DLT platform will be considered as credits and debits of accounts.

2. Banque de France is skeptical on the possibility for permissioned networks to qualify as
   ‘settlement internalisers’, as this notion is used in the CSDR to describe the execution of transfer
   of orders by an ‘institution’ (please refer to Article 2.1(11) of the CSDR), which is understood to be
   read as a reference to the notion of ‘institution’ under the SFD, which excludes the provider of the
   technical infrastructure used by participants. This understanding goes in favour of considering
   permissioned networks as system operators, and hence of the designation as ‘systems’ under the
   SFD. Only participants to the ‘system’ (or their clients as the case may be) can be considered as
   ‘settlement internalisers’.

---

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

- Yes
- No
- Don’t know/no opinion

Please explain your reasoning.
Banque de France is of the opinion that book-entry requirements under CSDR would be compatible with security tokens, provided that records on a DLT would be recognized as book-entries by relevant piece of legislation. Security tokens are a kind of dematerialization that goes beyond dematerialization currently practiced by CSDs. If, under the applicable law, records on a DLT cannot be legally qualified as securities accounts, book-entry requirements under CSDR are compatible with security tokens if records on a DLT were specifically recognized as book-entries by the law.

Article 3(2) of the CSDR requires that securities traded on a venue within the meaning of MiFID be recorded in book-entry form in a CSD, the securities account being defined as being an “account on which securities may be credited or debited”. We welcome in this respect ESMA’s January 2019 opinion on ICOs and crypto-assets, whereby ESMA considers that the CSDR is not prescriptive regarding the nature of the recording on an account with the central depository. In light of Recital 11 according to which the Regulation does not intend to “impose one particular method for the initial book-entry recording, which should be able to take the form of immobilisation or of immediate dematerialisation”, ESMA considers that it is incumbent on national law to indicate the form that could be taken by recording on an account, including on a blockchain. The only constraint imposed by the regulation is that this recording on an account should take place via an authorised central depository.

The CSDR therefore does not oppose the recording of security tokens in the central depository taking place via a blockchain and not via an account as understood from an accounting viewpoint. This calls an explicit legal clarification through a definition of ‘book entry’ and ‘dematerialized form’, in the SFD and / or in the CSDR (with possible cross-references).

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.

The French legislation, wishing to foster the emergence of new technologies in France and taking due account of segments not covered by CSDR, has taken steps to amend the Monetary and Financial Code and the Commercial Code. The French Monetary and Financial Code (MFC) explicitly foresees the possibility to recourse to DLT for the settlement of securities that do not fall under CSDR requirements (in particular commercial paper and securities that are not traded nor admitted to trading) and provides for the transfer of ownership when securities are recorded on a DLT.

The French Government has published a “Blockchain Order” in December 2017 (n° 2017-167) that « Allow the representation and transfer, by means of a DLT, of financial securities which are not admitted to the operations of a CSD or delivered in a securities settlement system ». The scope of this regulation is applicable to: (i) non-listed securities: (i) negotiable debt instruments, (ii) units or shares of investment funds and (iii) shares issued by joint-stock companies and debt instruments others than negotiable debt instruments which are not traded on a trading venue. This Order facilitates the use of DLT solutions since it creates legal comfort for actors developing projects.

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

<table>
<thead>
<tr>
<th>Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>X</td>
<td>No opinion</td>
</tr>
<tr>
<td>Rules on measures to prevent settlement fails</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organisational requirements for CSDs</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules on outsourcing of services or activities to a third party</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules on communication procedures with market participants and other market infrastructures</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules on the protection of securities of participants and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Please explain your reasoning (if needed).

Some existing rules cannot be applied as such to DLTs and will need to be adapted. Certain requirements (cybersecurity, minimal requirements for public and private keys) should be introduced in the current legislation that do not need to apply to CSDs. On the other hand, some rules, such as for example the rules on CSD links might not be applicable to DLTs as such, for technical reasons.

To specify further details:

Settlement periods: We have not identified any issues regarding the settlement period of two business days after the trading took place, imposed by CSDR. Indeed, a DLT is supposed to allow a real-time settlement (although it remains some issues with regards to the settlement of the cash leg, which would have to be achieved through the traditional banking circuit until no central bank money or commercial money may circulate in the DLT).

Settlement fails: We have not identified any major issues regarding to rules governing settlement fails in CSDR. However, some of those rules could be adapted could be adapted if settlement discipline rules prove unnecessary on the blockchain.

In particular, Article 2 of Delegated Regulation no. 2018/1229 of 25 May 2018 imposes on professional clients, upon settlement fails, to send to the relevant investment firm written allocations specifying notably “the names and numbers of the securities or cash accounts to be credited or debited.” Such specification might be to some extent inconvenient to apply in a DLT environment which does not reflect the features of traditional cash and securities accounts. We think this article should be broadened to encompass the specificities of DLT.

Organisational requirements for CSD: Please see our developments above in our response to question 88 (paragraph “Central Securities Depository operating rules”) reproduced below:

Central Securities Depository operating rules: The CSDR imposes numerous operating rules on central securities depositories (requirements which should be complied with by the managers of blockchains performing the settlement system function), which would not be unfeasible for security token platforms but which could be disproportionate due to the costs they entail: organisational requirements (rules of good conduct, robust governance, provisions relating to managers and personnel, conflicts of interests, reporting of offences, independent audit), settlement discipline (rules applicable in the case of default by a participant), supervision, issuance integrity, and protection of securities (asset segregation). It is likely that these obligations will have to be adapted to allow for the specific characteristics of the blockchain for which technology is likely to ensure greater security in transactions. Apart from the costs, these requirements might be unuseful for the way in which the blockchain operates (unfalsifiable distributed ledger, smart contracts).
Rules on outsourcing of services or activities to a third-party: no incompatibility identified.

Rules on communication procedures with market participants and other market infrastructures: no incompatibility identified.

Rules on the protection of securities of participants and those of their clients: Article 38 of CSDR on the protection of securities of participants and those of their clients imposes that the CSD be able to segregate in the accounts with the CSD, the securities of a participant from those of any other participant and, if applicable, from the CSD’s own assets. The CSD must also enable the participants to segregate the securities of the participant from those of the participant’s clients, and upon demand of a client, the securities of a participant from those of another participant.

DLT would not in itself allow a proper segregation of “securities accounts” as in the traditional system. However, in the DLT environment, the public address (key) of a client would, would consequently show, on the basis of the transactions that are registered on the blockchain, how many securities such client owns. In this regard, since a segregation is automatically done via the blockchain system, the segregation obligations of CSDR might not be relevant per se in a DLT environment.

Plus, a definition of OSA/ISA accounts (see § 3 and 4 of Article 38 of CSDR) in a DLT environment would need to be investigated (for instance, would the activity of holding the private keys on behalf of a client equates to the holding of a securities account on behalf of such client within the meaning of CSDR?)

Rules regarding the integrity of the issue and appropriate reconciliation measures:

Article 59 of delegated regulation no. 2017/392 of CSDR provides that “A CSD shall use double-entry accounting, according to which for each credit entry made on a securities account maintained by the CSD, centrally or not centrally, there is a corresponding debit entry on another securities account maintained by the same CSD.” Reconciliation measures set out by CSDR lean on the existence of two securities accounts. Then, except if we consider that the securities account is the public address of the client (which could otherwise raise some legal difficulties), this text cannot literally be applied in a DLT environment.

Rules on cash settlement: please see our response to question 88 above, paragraph “Cash settlement"reproduced below:

Article 40 of the CSDR provides that "For transactions denominated in the currency of the country where the settlement takes place, a CSD shall settle the cash payments of its securities settlement system through accounts opened with a central bank of issue of the relevant currency where practical and available." The second paragraph specifies that "Where it is not practical and available to settle in central bank accounts as provided in paragraph 1, a CSD may offer to settle the cash payments for all or part of its securities settlement systems through accounts opened with a credit institution or through its own accounts."

If cash is defined as scriptural money, there are three possibilities for settlement of the security tokens delivered on a blockchain operated by a central securities depository:

- Settlement is performed in fiduciary money via accounts opened with a central bank (paragraph 1 of Article 40). In this case, if delivery of the security tokens takes place on the blockchain, settlement, for its part, takes place in the conventional banking circuit, directly in central bank money;

- Settlement is performed in commercial money via the accounts of the central securities depository or via accounts opened with a credit institution (paragraph 2 of Article 40). In the same way, as things stand at present, the settlement of securities could not be performed directly on the blockchain but through the conventional banking system;

It could be considered that when transactions are denominated in cryptocurrency, they evade the scope of application of Article 40 and are therefore exempted from cash settlement. Indeed, the first phrase of paragraph 1 of Article 40 refers only to “transactions denominated in the currency of the country where the settlement takes place”. This innovative interpretation of the text could produce real effects only if it were endorsed by the European Commission.
In the current state of the legislation, it would seem that the complete tokenisation of the settlement and delivery of security tokens is impossible. Although the delivery of security tokens could be performed on a blockchain operated by a central securities depository authorised for this purpose, settlement, meanwhile, would in theory have to take place in fiduciary money and not in cryptocurrency. This would therefore require the central securities depository to effect movements in its cash accounts at the same time as the blockchain, which to some extent limits the productivity gains that can be expected from the tokenisation of post-trade infrastructures. A legislative adaptation of the CSDR seems necessary to allow settlement in cryptocurrency unless the European Central Bank decided to issue central bank money on a blockchain.

No issues have been identified with respect to rules on requirements for participation, requirements for CSD links and access between CSDs and access between a CSD and another market infrastructure as DLT would not impact such mechanisms.

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? Please explain your reasoning.

In the current state of French legislation, book-entry form in the central securities depository is not equivalent to a deed of ownership. This is obtained only by recording on an account with a custodian. As things stand at present, it would therefore be necessary for security token platforms to go through another intermediary in addition to the central securities depository – the custodian– who would record the security token transfers in its accounts to reflect their transmission on the blockchain. This possibility, which is the only one conceivable at present to secure the transfer of rights of ownership to security tokens, would however not make it possible to benefit fully from the productivity gains made possible by the blockchain.


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.

93) Would you see any particular issue (legal, operational, technical) with applying the following definitions in the SFD or its transpositions into national law in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

<table>
<thead>
<tr>
<th>Definition</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>definition of a securities settlement system</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>definition of system operator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>definition of participant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>definition of institution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>definition of transfer order</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>what could constitute a settlement account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>what could constitute collateral security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

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

70 Settlement Finality Directive (98/26/EC)
Please explain your reasoning.

We are of the view that the main definitions of the SFD should be adapted to a DLT environment.

As a general remark, EU law could make a distinction between securities settlement systems and DLTs since they do not have the same governance and review all these definitions in order to clarify whether they can be applied as such to DLTs or whether they need to be adapted. This being said, participants and transfer orders should be considered on equal terms to ensure that SFD requirements are met by all economic operators, SSS and DLTs.

In particular, the issues identified in the SFD are as follows:

Definition of a securities settlement system: As regards to the definition of “system”, we do not think that such definition is in itself incompatible with the DLT.

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

The definition of a securities settlement system has been transposed to Article L. 330-1 of the Monetary and Financial Code. This definition does not seem incompatible with settlement on a blockchain. The law provides that a settlement and delivery system is either instituted by a public authority, or "governed by a framework agreement that respects the general principles of a market framework agreement or a model agreement". At first sight, there is apparently nothing to prevent the settlement and delivery of security tokens from taking place on a blockchain recognised as a securities settlement system and reported as such to ESMA. However, it should be examined to what extent a public blockchain could be recognised as a securities settlement system.

Definition of system operator: The definition of “system operator” as the entity or entities legally responsible for the operations of the systems could raise issues in the context of public blockchains. Please see our response to question 88 paragraph “identification of a system manager”.

Definition of participant/institution: A securities settlement system must have a manager who is the person who applies for the central depository authorisation. However, as mentioned earlier, platforms of a hybrid or decentralised nature (transaction execution on the blockchain) which are based on public blockchains do not have a manager (analysis on a case-by-case basis for hybrid platforms). Only some of the centralised security token platforms could develop within the current legal framework. In practice, the obligation of having a manager excludes the use of public blockchains insofar as no manager can take responsibility for the completely orderly functioning of the blockchain. An analysis ought to be made to see how to classify the use of a permitted public blockchain (use of the underlying blockchain technology but enacting of specific operating rules by a service provider).

Definition of transfer orders: transfer orders in the SFD target both (i) the instructions by a participant to transfer the title to or the interest in a security and (ii) the instructions by a participant to place at the disposal of a recipient an amount of money (corresponding to the value of the securities bought) on the accounts of a credit institution, central bank, CCP or settlement agent or discharge of a payment obligation as defined by the rules of the system. We could perfectly, from a legal standpoint, consider that the discharge of a payment obligation could be made in assets which are not central bank money. This definition of transfer orders in the SFD does not appear, in itself, incompatible with the DLT.
Definition of settlement account: Settlement accounts in the SFD refer to accounts which are held at a central bank, a settlement agent or a CCP to hold funds or securities. This definition not only involves a limited range of potential account-holders, but also limitedly refers to “funds”. At this stage, it is therefore not applicable in a DLT environment.

Definition of collateral security: We have not identified any issues as regard to the application of such definition in a DLT environment.

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? Please explain your reasoning.

Yes. The definition of “system” set out in Article 2 of SFD provides that the system shall be governed by the law of the Member State chose by the participants. Only the law of a Member State in which one of the participants has its head office may be chosen. In case of public blockchains, participants (legal and natural persons) can be numerous and scattered. Furthermore, since there is no “relevant account” in a DLT environment and since its localization would be difficult. In this respect the conditions of designation of the applicable law could raise operational issues.

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?

With regard to securities that are not admitted to the operations of a CSD, the French Blockchain Order of 2017 allows certain securities to be issued and transmitted on the blockchain. The scope of the Blockchain Order has been intentionally limited to financial securities which are not subject to the European legislation (CSDR), i.e. mainly securities which are in registered form. In practice, this include:

- equity securities and debt securities issued by joint-stock companies not traded on a trading venue within the meaning of MiFID II;
- units or shares in collective investment undertakings not admitted to the operations of a central depository;
- negotiable debt securities.

The register of these securities can be kept in a shared electronic recording system (subject to the constraints described in detail below) and the securities do not have to be recorded on an account with the central depository.

The Blockchain Order therefore already makes it possible to issue and transfer security tokens in the form of units or shares in CIUs not admitted to the operations of a central depository, negotiable debt securities, and equities and bonds not traded on a trading venue within the meaning of MiFID (in practice OTC and brokerage platforms). For unlisted securities within the scope of the Blockchain Order, settlement and delivery can already be performed on the blockchain without any legal problem.

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

If yes, please provide specific examples (e.g. provisions national legislation transposing or implementing SFD, supervisory practices, interpretation, application…). Please explain your reasoning. [Insert text box]
In Banque de France’s opinion, if SFD does not constitute a legal barrier to security tokens, the current wording of the SFD is not adapted to DLTs. It should be adapted in order to apply its provisions to DLT. If adapted, its provisions, and notably the legal certainty on the rights and obligations of entities involved in a financial transaction at each stage before effective settlement (in particular moments of entry and irrevocability), and the possibility for participants to apply derogations to the ordinary insolvency rules, would probably act as an important factor to encourage further recourse to DLT.

7. Financial Collateral Directive (FCD)

The Financial Collateral Directive\(^72\) aims to create a clear uniform EU legal framework for the use of securities, cash and credit claims as collateral in financial transactions. Financial collateral is the property provided by a borrower to a lender to minimise the risk of financial loss to the lender if the borrower fails to meet their financial obligations to the lender. DLT can present some challenges as regards the application of FCD. For instance, collateral that is provided without title transfer, i.e. pledge or other form of security financial collateral as defined in the FCD, needs to be enforceable in a distributed ledger\(^73\).

97) Would you see any particular issue (legal, operational, technical) with applying the following definitions in the FCD or its transpositions into national law in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for “not a concern” and 5 for “strong concern”.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>if crypto-assets qualify as assets that can be subject to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>financial collateral arrangements as defined in the FCD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>if crypto-assets qualify as book-entry securities collateral</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

\(^71\) In particular with regard to the question according to which criteria the location of the register or account should be determined and thus which Member State would be considered the Member State in which the register or account, where the relevant entries are made, is maintained.

\(^72\) Financial Collateral Directive (2002/47/EC)

\(^73\) ECB Advisory Group on market infrastructures for securities and collateral, “the potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration” (2017)
Please explain your reasoning.

In our view, there is no provisions in the FCD that would fully prevent a crypto-asset (a security token) to be subject to financial collateral.

Further, to the extent that the definition of “book-entry securities collateral” merely indicates that it shall be evidenced by “entries in a register”, such definition would be compatible with DLT.

Relevant account is defined as a “register or account […] in which the entries are made by which that book-entry securities collateral is provided to the collateral taker. This definition seems compatible with the FCD if we consider that the blockchain is the register (this is subject to certain discrepancies with CSDR if we consider that the blockchain constitutes the securities account).

However, there might be a need for clarification to address several legal and operational/technical issues related to the use of crypto-assets as collateral in financial transactions, in particular: operationally, how can the collateral rights on crypto-assets be materialized/identified? Technically, how can the collateral taker be able to realise the collateral if need be? Technically, how can any reuse right be organised on a DLT? Legally, how can the “relevant account” be localised (whereas our understanding is that there is no account but a DLT)?

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

The main rule on conflict of laws set out in FCD relies on the notion of “relevant account”. A DLT environment is not “an account”, so the conflict of laws rule would have to be expanded and adapted to DLT. The lex rei sitae defined by the above-mentioned directive remains accurate, but shall be further assessed. Reference could be made to the operator of the blockchain - but such approach would be insufficient in respect of public blockchains – or to the key holding, if the activity of holding the private keys on behalf of a client equates to the holding of a securities account.

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?

FCD rules as transposed in the French Monetary and Financial Code establish an exemption to French insolvency proceedings set out in Book VI of the French Commercial Code. All guarantees that are not in the scope of FCD would therefore be subject to French rules applicable in case of insolvency of the collateral giver or collateral taker.

Still, we have not been confronted to this issue (which may be complex) so far.

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

If yes, please provide specific examples (e.g. provisions national legislation transposing or implementing FCD, supervisory practices, interpretation, application…). Please explain your reasoning.
No, we do not think that the use of DLT solution would be limited by the FCD, even if some difficulties may appear during implementation that would need clarification (See examples above in questions 97 and 98).

Note that the French Blockchain Order already mentioned above allows to pledge securities that are not admitted to the operations of a CSD in a DLT.

8. European Markets Infrastructure Regulation (EMIR)

The European Markets Infrastructure Regulation (EMIR)\textsuperscript{75} applies to the central clearing, reporting and risk mitigation of over-the-counter (OTC) derivatives, the clearing obligation for certain OTC derivatives, the central clearing by central counterparties (CCPs) of contracts traded on financial markets (including bonds, shares, OTC derivatives, Exchange-Traded Derivatives, repos and securities lending transactions) and services and activities of CCPs and trade repositories (TRs).

The central clearing obligation of EMIR concerns only certain OTC derivatives. MiFIR extends the clearing obligation by CCPs to regulated markets for exchange-traded derivatives. At this 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.

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

\textsuperscript{75} European Markets Infrastructure Regulation (648/2012/EU)
101) Do you think that security tokens are suitable for central clearing?

<table>
<thead>
<tr>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely appropriate</td>
</tr>
<tr>
<td>Rather appropriate</td>
</tr>
<tr>
<td>Neutral</td>
</tr>
<tr>
<td>Rather inappropriate</td>
</tr>
<tr>
<td>Completely inappropriate</td>
</tr>
<tr>
<td>Don't know / No opinion</td>
</tr>
</tbody>
</table>

Please explain your reasoning (if needed).

Neutral to rather inappropriate. The transfer of the legal obligations linked to the crypto-assets from the market participant to the CCP through the novation seems at first sight complicated to implement technically. The central clearing of security tokens would require sending instructions and information to CCPs in a format that can be read and easily used by CCPs, which would require significant technical challenges for existing CCPs. Beyond these technical aspects, application of CCPs’ credit risk and liquidity risk models has so far remained unexplored, perhaps because of the high complexity entailed. Banque de France expects that central clearing will be the ultimate field of post-market activities to test, once confidence is gained on settlement of cash transactions and securities transactions. The involvement of multiple counterparties, the adequate calibration and management of pre-financed resources and adaptation of operational processes to a DLT environment will most probably only occur at best when security tokens are considered as fungible assets among other financial instruments (pending legal clarification in Mifid but also actual operational embedding).

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

<table>
<thead>
<tr>
<th>Issue</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules on margin requirements, collateral requirements and</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>requirements regarding the CCP’s investment policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules on settlement</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organisational requirements for CCPs and for TRs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Rules on segregation and portability of clearing members’ and clients’</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>assets and positions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules on requirements for participation</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting requirements</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (including other provisions of EMIR, national rules applying</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>the EU acquis, supervisory practices, interpretation, applications…</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

There are some issues with applying certain EMIR rules in a DLT environment.

Central clearing relies on the concept of an entity which, beyond calculating net positions, becomes the new counterparty to its clearing members i.e. replacing one bilateral contractual relationships with 2 opposing contracts with the CCP. Only permissioned networks and centralized platforms
can therefore be considered as possible ways to apply current rules in a DLT environment.

Recourse to permissioned ledgers and centralized platforms by CCPs is considered technically challenging due to the complex set-up of DLT which would be necessary for the sound and effective management of risks by CCPs (integration of risk models, initial and variation margin calls, segregation and portability of clearing members’ and clients’ assets and positions, efficient process of clearing members’ defaults…).

In details:

Margin requirements, collateral requirements and requirements regarding the CCP’s investment policy: In the absence of a CCP in a DLT system, such rules would be irrelevant. Further, margin and collateral requirements are based on the existence of clearing members which are subject to financial resources and operational capacity requirements. Again, this obligation of intermediation does not seem fully compatible with the functioning of crypto-asset platforms that rely on retail investors’ direct access.

However, the question whether the CCP could perform some of its functions (margin calls and collateral calls) via DLT solutions would besides have to be investigated. It is in this regard likely that smart contracts generated in a blockchain would allow to fulfill the requirements on margin and collateral. In this regard, provisions of EMIR (article 41 of EMIR, Article 24 of delegated regulation no. 153/2013) would possibly need to be adapted to welcome DLT solutions.

Rules on settlement: A CCP must settle its transactions in FIAT money, and if practicable and available, in central bank money. The issue regarding the settlement of transaction in FIAT money in a DLT has been addressed above (please see pages [66-67]).

Organisational requirements for CCPs and for TRs: Organisational requirements for CCP (governance requirements, risk management requirements, management of conflicts of interests, information to competent authorities) appear, as of today, disproportionate as compared to the size and financial capacities of the current actors in the DLT environment.

Furthermore, such requirements appear inappropriate for the way in which the blockchain operates (unfalsifiable distributed ledger, smart contracts) and in the fact that the DLT allows to settle transactions in real-time and on a gross basis. Such requirements would however not be an issue if already existing CCPs perform some of their functions (margin calls and collateral calls mainly) via DLT solutions.

Rules on segregation and portability of clearing members’ and clients’ assets and positions: the AMF does not view this obligation as applicable in a DLT environment to the extent that no proper clearing function would be assumed in the DLT.

Rules on requirements for participation: As regards requirements for participation, the French Monetary and Financial Code (in compliance with the SFD) sets a limitative list of categories of legal entities that can become clearing members. The technical set up of most DLTs will probably require fine tunings in order to restrict direct access. A broadening of direct access to new categories of legal or natural persons may be hindered by French law, according to which property rights over securities lie with securities accounts held by custodians. Furthermore, recent experience of the management of a natural person’s default by a European CCP clearly showed the high risks associated to a broad acceptance of entities as clearing members.

Reporting requirements: We have not identified any issues with the obligation of reporting to a TR set out in Article 9 of EMIR.
103) Would you see the need to clarify that DLT solutions including permissioned blockchain can be used within CCPs or TRs? [Insert text box]

No, not necessarily. In the field of CCPs and TRs, DLT solutions are already being explored as a technical solution to improve operational efficiency. The current regulation does not explicitly prevent market infrastructures to develop DLT solutions, as long as they meet the essential requirements especially regarding operational soundness and resilience. However, clarifications on the scope of the activities of the CCP that can be performed via DLT solutions and the conditions under which those activities should be performed could be welcomed.

104) Would you see any particular issue with applying the current rules to derivatives the underlying of which are crypto assets, in particular considering their suitability for central clearing? Please explain your reasoning (if needed). [insert text box]

From a theoretical perspective, there is no particular difference between a derivative (swap, future, option) on a crypto asset and a derivative contract referencing a different underlying. As long as the price of the underlying and the characteristics of the contract (swap, future, option) are known, the behavior of a derivative contract is standard, regardless of the underlying nature. Yet, to be suitable for clearing, several conditions would need to be met, namely:

(i) Reliability of price sources: for the CCP to be able to daily mark the contract to market, and to calculate initial margins, it needs to have access to one or several sources for the prices of the underlying, which is not always easy in the crypto-asset world.

(ii) Liquidity: to ensure that the CCP will be able to manage the default of a participant and liquidate its portfolio of derivatives, crypto-assets derivatives will need to be sufficiently liquid.

(iii) Physical settlement: most crypto-assets derivatives are currently cash settled. Development of physical settlement for crypto assets derivatives represents a challenge, as the platform / the CCP would need to manage the custody risk inherent to crypto-assets.


The Alternative Investment Fund Managers Directive76 (AIFMD) lays down the rules for the authorisation, ongoing operation and transparency of the managers of alternative investment funds (AIFMs) which manage and/or market alternative investment funds (AIFs) in the EU.

---

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

105) Do the provisions of the EU AIFMD legal framework in the following areas are appropriately suited for the effective functioning of DLT solutions and the use of security tokens? Please rate each proposal from 1 to 5, 1 standing for "not suited" and 5 for "very suited".

<table>
<thead>
<tr>
<th>Area</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

- Yes
- No
- Don’t know/no opinion

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

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.

107) Do the provisions of the EU UCITS Directive legal framework in the following areas are appropriately suited for the effective functioning of DLT solutions and the use of security tokens? Please rate each proposal from 1 to 5, 1 standing for "not suited" and 5 for "very suited".

<table>
<thead>
<tr>
<th>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&quot; and/or “transferable security”</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>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;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclosure and reporting requirements set out in the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11. Other final comments and questions as regards security tokens

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

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

- Yes
- No
- Don’t know/no opinion

If yes, please explain the regulatory approach that you favour. Please explain your reasoning (if needed).

Flexibility may be needed to allow innovation but should not lead to legal uncertainty which is strongly needed in trading and post-trading and to legal and operational risks.

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

The question deserves a reflection based on concrete examples to assess correctly the risks. Permissionless blockchains are more decentralized and by way of consequence more secure from a cyber point of view, but also in the quality of the underlying code, the robustness of which is tested on a larger scale. They may also give rise to other types of risks (such as the risk of fork for instance) that are less prevalent when there is a reduced number of participants to the network who trust and know each other.

We consider essential to make sure the regulatory framework remains technologically neutral.

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

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

- Yes
- No
- Don’t know/no opinion

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

It seems difficult to answer this question when in fact this regulatory separation exists. We faced a "chicken and egg" paradox: such a regulatory change would need to be documented with experience feedback, yet these same texts prevent the emergence of such projects. In the event that the EU agrees to set up a digital laboratory, the fact of having an integrated post-trade market place could be tested in order to be able to assess the risks and benefits of such a scheme.
111) Have you detected any issues beyond those raised in previous questions on specific provisions that would prevent effectively applying EU regulations to security tokens and transacting in a DLT environment, in particular as regards the objective of investor protection, financial stability and market integrity? [Insert text box]

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

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

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

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

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

C. Assessment of legislation for ‘e-money tokens’

Electronic money (e-money) is a digital alternative to cash. It allows users to make cashless payments with money stored on a card or a phone, or over the internet. The e-money directive (EMD2)\(^{78}\) sets out the rules for the business practices and supervision of e-money institutions.

In its advice on crypto-assets\(^{79}\), the EBA noted that national competent authorities reported a handful of cases where payment tokens could qualify as e-money, e.g. tokens pegged to a given currency and redeemable at par value at any time. Even though such cases may seem limited, there is merit in ensuring whether the existing rules are suitable for these tokens. In that this section, payments tokens, and more precisely “stablecoins”, that qualify as e-money are called ‘e-money tokens’ for the purpose of this consultation. Consequently, firms issuing such e-money tokens should ensure they have the relevant authorisations and follow requirements under EMD2.

Beyond EMD2, payment services related to e-money tokens would also be covered by the Payment Services Directive\(^ {80}\) (PSD2). PSD2 puts in place comprehensive rules for payment services, and payment transactions. In particular, the Directive sets out rules concerning a) strict security requirements for electronic payments and the protection of consumers’ financial data, guaranteeing safe authentication and reducing the risk of fraud; b) the

\(^{79}\) EBA report with advice for the European Commission on “crypto-assets”, January 2019  
\(^{80}\) Payment Services Directive 2 (2015/2366/EU)
transparency of conditions and information requirements for payment services; c) the rights and obligations of users and providers of payment services.

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

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

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

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

If the question referred to e-money token that meets the definition of e-money set by EMD2 (see explanation in section C) as illustrated in the EBA report, in principle EMD2 requirements can’t constitute impediments to the effective functioning of e-money token.

However globally speaking, EMD2 defines electronic money as “ectronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer”. Similarly, French law defines electronic money as a ‘monetary value which is stored in a digital format, including a magnetic format, which represents a claim on the issuer, that is issued on receipt of funds for payment transactions’ purposes, and which is accepted by a natural or legal person other than the electronic money issuer’ (article L.315-1 of the French monetary and financial code).

As blockchain and other distributed ledger technology (DLT) are electronic recording device, “e-money tokens” may be fully subject to EMD2 providing they respect the other criteria defined by EMD2. However, in our opinion, the ‘e-money' definition under EMD2 excludes most crypto-assets.

The use cases behind such “e-money token” are hardly grasped by EMD2 as the issuance of the token is effectively operated by the nodes. Furthermore, even where a single entity defines the governing rules of the issuance and is ultimately responsible for it, the tokens may not represent a claim on this entity. Indeed, some crypto-assets do not grant the crypto-asset holder a claim onto the crypto-asset issuer. It is our understanding that crypto-assets that do not embed such a claim right on the issuer would not qualify as ‘e-money’.

Against this background, and although no elements of EMD2 constitute impediments per se to the effective functioning or use of “e-money tokens”, we must stress that crypto-assets would rarely qualify as “e-money” under the current legal framework.

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, but some actors may need to ask both for PSP license and for crypto-asset provider license might be an issue.

As already stated in question 36, PSD2 defines a payment transaction as ‘an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee’ (article 4.5 of PSD2). Indeed, most payment services (except account information service) imply that funds are being or will be transferred from the payer’s payment account to a payee’s payment account.

In our view, the definition of ‘payment transaction’ under PSD2 might apply to some crypto-asset transactions. For instance, when a crypto-asset service provider acquires a payment transaction in euros and buys a crypto-asset on behalf of its customer and then sell that crypto-asset back to its client thereby executing a payment transaction for their client (see question 36). In our understanding, such an operation would require crypto-assets withholding third party’s funds to be licensed as payment service provider. However, intermediaries buying and selling crypto-assets on own account would not be subject to such license requirement.

Nonetheless, the requirement to hold both a license for ‘payment services’ and a license for ‘crypto-asset services’ might introduce too much regulatory constraints on smaller crypto-asset service providers. Therefore, if a bespoke regime was to be set up, it could authorize ‘crypto-asset service providers’ to carry out ‘payment services linked with crypto-asset services’ if they abide by adequate prudential requirements. The definition of ‘linked payment services’ might be similar to what was drafted for payment transaction related to securities asset servicing under article 3 (i) PSD2.

115) In your view, do EMD2 or PSD2 require legal amendments and/or supervisory guidance (or other non-legislative actions) to ensure the effective functioning and use of e-money tokens?

- Yes
- No
- Don’t know/no opinion

Please provide specific examples and explain your reasoning (if needed).

Yes.

EMD 2 legal amendments
As a preliminary remark and as already stated in question 113, whether tokens qualify as “e-money” must be clarified, as EMD2 would exclude this possibility for most crypto-assets. The crypto-assets should meet all the criteria defined under its article 2.2 to qualify as ‘e-money’. The main limitation to such qualification under the current legal framework is that it remains to be
ascertained on a case-by-case basis whether a specific crypto-asset represents a claim on its issuer.

If they were to qualify as ‘e-money’, the current development trend of the DLTs and the issuance of such tokens may lead to an increased number of licensed EMI. In this context of growth of exchanges in the form of ‘e-money tokens’, it is critical that the risks borne by those entities are accurately reflected in the requirements laid under EMI anti money laundering and terrorist financing (AML-TF) regime and own funds regime. In that regard, we stress that, under the current applicable legal framework, market participants may construct their activity in such a way that arbitrage between electronic money institution (EMI) and payment institution (PI) licenses are possible for borderline use cases.

Firstly, where the entity executes large volumes of payment transaction, an EMI license may be less demanding than a PI license. Pursuant Article 5 (3) EMD2, the own funds of an electronic money institution for the activity of issuing electronic money amounts to at least 2% of the average outstanding electronic money. However, where an e-money token is used for the purpose of exchanges such as in peer-to-peer payments (closely similar to remittance models), there is a rapid issuance and reimbursement cycle. As such, the outstanding amount of electronic money is mechanically kept a low level because the e-money is rapidly reimbursed which translate into low requirements on own funds. We believe that in such models, EMD2 does not fully encompass the risks borne by the issuer because it mostly derives from the execution of the transactions and not from the outstanding amount of e-money token. Therefore, the volume of transactions should be taken into account in a similar fashion as PSD2 does in method B (article 9 (1) PSD2).

Secondly, the current applicable regime to prevent the use of e-money systems for the purpose of money laundering and terrorist financing should be amended to converge with the payment service regime in order to promote a sounder ecosystem. Indeed, where some conditions are met, mostly if the amount stored electronically (i.e. the e-money token) does not exceed EUR 250 (recently lowered to EUR 150), the simplified customer due diligence regime for EMI allows them not to apply certain KYC measures. This situation may distort the robustness of the EU AML-FT program as market participants may seek to qualify as EMI only to avoid KYC costs although their activity has a similar risk profile as PI. To avoid such arbitrage, we also believe that the threshold should be reviewed to fully grasp the risk of e-money tokens used for exchange purposes. Against this background, we propose to work on an evolution of EMD2 that would ensure the protection of the consumers and the financial system and that would converge towards the prudential requirements of PSD2.

PSD2 legal amendments
As specified on our answer to question 36, the notion of ‘payment transactions’ and more specifically its reference to the notion of ‘funds’ should be clarified to determine whether a payment transaction could involve an exchange of crypto-assets. If the answer were to be positive, then ‘crypto-asset service providers’ storing and selling/buying crypto-assets on behalf of third parties would have to be licensed as payment service providers.

As previously outlined, holding both this license and a license for ‘crypto-asset services’ might introduce too much regulatory constraints and limit the policy effect of the crypto-asset framework. Therefore, if a bespoke regime was to be set up, it could authorize ‘crypto-asset service providers’ to carry out specific ‘payment services’ provided they are intrinsically linked with the selling/buying activity. We stress that such a bespoke regime would require a careful risk-based approach.
Under EMD 2, electronic money means ‘electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […] and which is accepted by a natural or legal person other than the electronic money issuer’. As some “stablecoins” with global reach (the so-called “global stablecoins”) may qualify as e-money, the requirements under EMD2 would apply. Entities in a “global stablecoins” arrangement (that qualify as e-money under EMD2) could also be subject to the provisions of PSD2. The following questions aim to determine whether the EMD2 and/or PSD2 requirements would be fit for purpose for such “global stablecoin” arrangements that could pose systemic risks.

116) Do you think the requirements under EMD2 would be appropriate for “global stablecoins” (i.e. those that reach global reach) qualifying as e-money tokens? Please rate each proposal from 1 to 5, 1 standing for "completely inappropriate" and 5 for "completely appropriate").

<table>
<thead>
<tr>
<th>Requirements</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial capital and ongoing funds</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safeguarding requirements</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issuance</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redeemability</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of agents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Out of court complaint and redress procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please explain your reasoning (if needed).

We consider that stable coins consist in an “asset-backed” issuance in so far as they are backed by a stock of underlying assets. Two challenges arise from this feature:

- Ensuring that the stock of underlying assets genuinely exists not only when the crypto-asset is issued but also throughout the crypto-asset’s life cycle.
- Ascertaining whether stable coin users possess a claim on the stable coins themselves and on their underlying assets.

For example, we believe that Libra could be considered as an asset-backed stable coin because its value is pegged to a basket of assets. Yet, Libra is largely similar to regulated payment activities such as issuing electronic money or providing payment services. Such a qualification would not however be fully satisfactory since these regulatory regimes would not fully encompass the business activities surrounding Libra. Indeed, these regimes were constructed to be voluntary less stringent than those applicable to other banking activities and were still intended to rigorously safeguard users’ funds. Capital requirements (350 000 €) for a licence of EMI is not relevant for an issuer of global stable coins (should be more important). If global stable coins can be used outside of EU, an EU legal text is not fully relevant to regulate one leg transactions. Consequently, these regimes would appear to be unsuitable for the size of Libra’s acceptance network.

The definition of e-money under the second Electronic Money Directive (EMD2) could be extended in order for stable coins to fit into the e-money definition. Consequently, stable coins’ issuers and service providers would have to abide by EMD2 prudential requirements, which we consider to be suitable for safeguarding stable coin users’ funds.
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)?

<table>
<thead>
<tr>
<th>Opinion</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Completely appropriate</td>
<td></td>
</tr>
<tr>
<td>Rather appropriate</td>
<td></td>
</tr>
<tr>
<td>Neutral</td>
<td>X</td>
</tr>
<tr>
<td>Rather inappropriate</td>
<td></td>
</tr>
<tr>
<td>Completely inappropriate</td>
<td></td>
</tr>
<tr>
<td>Don't know / No opinion</td>
<td></td>
</tr>
</tbody>
</table>

Please explain your reasoning (if needed).

Similarly, we are of the opinion that PSD2 prudential requirements would be adequate to oblige stable coin issuers and service providers to safeguard their clients’ funds. The definition of payment transactions might have to be amended in order to include stable coins’ specificities.

* *
* *
<table>
<thead>
<tr>
<th>Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AIF</strong> – Alternative Investment Fund</td>
</tr>
<tr>
<td><strong>AIFM</strong> – Alternative Investment Fund Manager</td>
</tr>
<tr>
<td><strong>AML/CFT</strong> – Anti-Money Laundering/ Combatting the Financing of Terrorism</td>
</tr>
<tr>
<td><strong>BCBS</strong> – Basel Committee on Banking Supervision</td>
</tr>
<tr>
<td><strong>CCP</strong> – Central Clearing Counterparty</td>
</tr>
<tr>
<td><strong>CDS</strong> – Credit Default Swap</td>
</tr>
<tr>
<td><strong>CSD</strong> – Central Securities Depositories</td>
</tr>
<tr>
<td><strong>CSDR</strong> – Central Securities Depositories Regulation (909/2014/EU)</td>
</tr>
<tr>
<td><strong>DLT</strong> – Distributed Ledger Technology</td>
</tr>
<tr>
<td><strong>DMD</strong> – Distance Marketing of Consumer Financial Services Directive (2002/65/EC)</td>
</tr>
<tr>
<td><strong>EBA</strong> – European Banking Authority</td>
</tr>
<tr>
<td><strong>ECB</strong> – European Central Bank</td>
</tr>
<tr>
<td><strong>EIOPA</strong> - European Insurance and Occupational Pensions Authority</td>
</tr>
<tr>
<td><strong>EMIR</strong> – European Markets Infrastructure Regulation (648/2012/EU)</td>
</tr>
<tr>
<td><strong>ESAs</strong> – European Supervisory Authorities (EBA, EIOPA, ESMA)</td>
</tr>
<tr>
<td><strong>ESCB</strong> – European System of Central Banks</td>
</tr>
<tr>
<td><strong>ESMA</strong> – European Securities Market Authority</td>
</tr>
<tr>
<td><strong>ETF</strong>– Exchange-Traded Fund</td>
</tr>
<tr>
<td><strong>EU</strong>- European Union</td>
</tr>
<tr>
<td><strong>FATF</strong> – Financial Action Task Force</td>
</tr>
<tr>
<td><strong>FCD</strong> – Financial Collateral Directive (2002/47/EC)</td>
</tr>
<tr>
<td><strong>FSB</strong> – Financial Stability Board</td>
</tr>
<tr>
<td><strong>ICO</strong> – Initial Coin Offering</td>
</tr>
<tr>
<td><strong>ICT</strong> – Information Communication Technologies</td>
</tr>
<tr>
<td><strong>IPO</strong> – Initial Public Offering</td>
</tr>
<tr>
<td><strong>ISIN</strong> – International Securities Identification Number</td>
</tr>
</tbody>
</table>
Definitions

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

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

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

**Distributed Ledger Technology (DLT):** means of saving information through a distributed ledger, i.e., a repeated digital copy of data available at multiple locations. DLT is built upon public-key cryptography, a cryptographic system that uses pairs of keys: public keys, which are publicly known and essential for identification, and private keys, which are kept secret and are used for authentication and encryption.
**Financial instrument:** those instruments specified in Section C of Annex I in MiFID II

**Electronic money (e-money):** ‘electronic money’ means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer;

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

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

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

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

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

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

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

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

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

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

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

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

**Stablecoins:** For the purpose of the consultation, “stablecoins” are considered as a form of payment tokens whose price is meant to remain stable through time. Those “stablecoins” are typically asset-backed by real assets or funds or by other crypto-assets. They can also take the form of algorithmic “stablecoins” (with algorithm being used as a way to stabilise volatility in the value of the coin).

**Trading venue:** Under MiFID Article 4(1)(24), trading venue means a regulated market, a multilateral trading facility, or an organised trading facility (OTF’).
**Virtual Currencies:** Under AMLD5, virtual currency means ‘digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically’.

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