



## EUROPEAN COMMISSION

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

### CONSULTATION DOCUMENT

On an EU framework for markets in crypto-assets

#### **Disclaimer**

This document is a working document of the Commission services for consultation and does not prejudice 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 **18 March 2020** at the latest to the online questionnaire available on the following webpage: XX

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: xxx

## INTRODUCTION:

### 1. Background for this public consultation

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

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

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

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

Crypto-assets are one of the major applications of blockchain for finance. Crypto-assets are commonly defined as a type of private assets that depend primarily on cryptography and distributed ledger technology as part of their inherent value<sup>2</sup>. For the purpose of this consultation, they will be defined as *"a digital asset that may depend on cryptography and exists on a distributed ledger"*. Thousands of crypto-assets, with different features and serving different functions, have been issued since Bitcoin was launched in 2009<sup>3</sup>. There are many ways to classify the different types of crypto assets<sup>4</sup>. 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

---

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

<sup>2</sup> [EBA report with advice for the European Commission on "crypto-assets"](#), January 2019

<sup>3</sup> ESMA, ['Advice on Initial Coin Offerings and Crypto-Assets'](#), January 2019

<sup>4</sup> See: ESMA Securities and Markets Stakeholder Group, Advice to ESMA, October 2018

companies (SMEs), by streamlining capital-raising processes and enhancing competition. The ‘tokenisation’ of traditional financial instruments is also expected to open up opportunities for efficiency improvements across the entire trade and post-trade value chain, contributing to more efficient risk management and pricing<sup>5</sup>. 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<sup>6</sup> 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<sup>7</sup>, 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<sup>8</sup>, 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<sup>9</sup>: (i) For crypto-assets that are covered by EU rules by virtue of qualifying as financial instruments under the Markets in financial instruments Directive<sup>10</sup> - MiFID II - or as electronic money/e-money under the Electronic Money Directive - EMD<sup>11</sup>, the

---

<sup>5</sup> 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.

<sup>6</sup> ESMA, [‘Advice on Initial Coin Offerings and Crypto-Assets’](#), January 2019; [EBA report with advice for the European Commission on “crypto-assets”](#), January 2019

<sup>7</sup> [FSB Chair’s letter to G20 Finance Ministers and Central Bank Governors](#), Financial Stability Board, 2018

<sup>8</sup> G7 Working group on ‘Stablecoins’, [Report on ‘Investigating the impact of global stablecoins’](#), October 2019

<sup>9</sup> [Speech by Vice-President Dombrovskis at the Bucharest Eurofi High-level Seminar](#), 4 April 2019

<sup>10</sup> [Market in Financial Instruments Directive](#) (2014/65/EU)

<sup>11</sup> [Electronic Money Directive](#) (2009/110/EC)

Commission services have screened EU legislation to assess whether it can be effectively applied. For crypto-assets that are currently not covered by the EU legislation, the Commission services are considering a possible proportionate common regulatory approach at EU level to address, *inter alia*, potential consumer/investor protection and market integrity concerns.

Given the recent developments in the crypto-asset market, the President of the Commission, Ursula von der Leyen, has stressed the need for *“a common approach with Member States on crypto-currencies to ensure we understand how to make the most of the opportunities they create and address the new risks they may pose”*<sup>12</sup>. 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”*<sup>13</sup>.

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

In this context and in line with Better Regulation principles<sup>14</sup>, 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<sup>15</sup>. 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**

---

<sup>12</sup> [Mission letter of President-elect Von der Leyen to Vice-President Dombrovskis](#), 10 September 2019

<sup>13</sup> Joint Statement of the European Commission and Council on ‘stablecoins’, 5 December 2019

<sup>14</sup> European Commission, [‘Better Regulation: Why and How’](#)

<sup>15</sup> 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).

**purpose of the consultation, those regulated crypto-assets are respectively called ‘security tokens’ and ‘e-money tokens’.** Responses will allow the Commission to assess the impact of possible changes to EU legislation (such as the Prospectus Regulation<sup>16</sup>, MIFID II, the Central Securities Depositories Regulation<sup>17</sup>...) 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 **18 March 2020**.

## **PUBLIC CONSULTATION**

### **I. Questions for the general public**

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

#### **1) Have you ever held crypto-assets?**

- Yes
- No

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

##### **2.1. Was it simple and straightforward to buy them?**

- simple
- neither easy nor hard
- complex

##### **2.2. Did you feel sufficiently well informed about your rights, the risks and opportunities?**

- Yes
- No

##### **2.3. Did you buy the crypto-assets from an EU or non-EU vendor, exchange or trading platform?**

- EU
- Non-EU
- Don’t know

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

- Yes

---

<sup>16</sup> [Prospectus Regulation](#) (2017/1129/EU)

<sup>17</sup> [Central Securities Depositories Regulation](#) (909/2014/EU)

- No

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

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

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

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

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

- Yes
- No

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

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

**Please explain the reasons why you are planning to hold crypto-assets (if needed).**

[Insert text box]

**4) If yes, in what timeframe?**

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

**II. Classification of crypto-assets<sup>18</sup>**

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'*<sup>19</sup> 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

---

<sup>18</sup> 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.

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

the Member States) can make it difficult for market participants to understand the obligations they are subject to. Therefore, a categorisation of crypto-assets is a key element to determine whether crypto-assets fall within the current perimeter of EU financial services legislation.

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

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

- [Yes](#)
- **No**
- **Don't know/no opinion**

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

Since the term "crypto-asset" is considered for the purpose of this survey as "*a digital asset that may depend on cryptography and exists on a distributed ledger*", it appears that the scope of this EU initiative should be limited to "crypto-assets" in order to allow a more "targeted effort". This definition also enables to include many forms of crypto-assets, and to capture all emerging crypto-asset types since crypto-assets represent a particularly moving market.

**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.

However, the AMF considers that giving a precise classification applied to crypto-assets could be premature at this stage. It is only after solid feedback that we will be able to judge the relevance of a precise classification (e.g. "utility tokens", security tokens", "payment tokens", "stablecoins" etc.).

At this stage, the AMF considers that these two key distinctions should be made:

- 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.

It allows for a broad category of crypto assets, most of which are limited in size and should be regulated as such. The responses of the AMF and recommendations for a bespoke regime with optional components are expressed in this perspective.

However, beyond this broad category of crypto-assets, it is extremely necessary to think about a specific way to deal with global stablecoins. The French authorities are very careful to put in place means to regulate these objects, and if necessary to prohibit them. To do so, there are two possibilities:

- Defining stablecoins and associate them with specific regulatory obligations. This proposal would allow a regulatory framework to apply to any stablecoin regardless of its size. However, this requires the ability to draw a line between stablecoins which would be concerned by mandatory requirements and other payment tokens only partially covered by mandatory requirements (e.g. AML CFT and fit and proper measures);
- Defining regulatory obligations for crypto-assets (whatever their form e.g. “utility tokens”, “payment tokens”, “stablecoins”) which reach global scale. This avoids drawing a line on the nature of the asset, but criteria will be needed to define the conditions under which an asset becomes global. It is important to keep in mind that a stablecoin can become a global stablecoin over time, which implies switching from one regime which could be partially optional to another which would be mandatory.

Beyond these points, due to the fact the market is very evolutive, we believe it is essential to make our regulatory frameworks and our supervisory practices more agile. Innovation could be hampered or driven outside the EU if we lock this new classification into overly strict and burdensome regulatory boxes. As the environment of crypto-assets is not mature, we are not in favor of a strict and definitive classification.

For the record, in France, crypto-assets are divided into two categories:

- crypto-assets for which financial regulation applies; and
- crypto-assets that fall outside the traditional EU regulations and are defined in France as “digital assets” in accordance with the French PACTE regime (see description below).

**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).**

As mentioned above in question 6, it is useful to draw a distinction between at least two types of crypto-assets: crypto-assets that are qualified as financial instruments and crypto-assets that do not fall within the definition of a financial instrument, those falling into the definition of electronic money and any token that would reach global scale or stablecoin, depending of the approach (see above), would have to be regulated specifically.

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

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

**Please explain your reasoning (if needed). If yes, indicate if any further sub-classification would be necessary.**

The traditional regulation de facto obliges the distinction between at least two types of crypto-assets: crypto-assets that are qualified as financial instruments and crypto-assets that do not fall within the definition of a financial instrument. We are not in favor of a more detailed classification (e.g. utility token, payment token, hybrid token, investment token, etc.), because it would bring more complexity, it would not give a clear and relevant picture of crypto-assets. For example, the scope of the definition of a “payment token” is unclear, as every crypto-asset can be used as a mean of payment. The same can be said for “investment tokens”: every token can be purchased as an investment vehicle. Further, definitions as “payment token”, “hybrid token” or “investment token” do not solve any problem. However, it would be relevant to consider “hybrid tokens” as financial instruments. Clarification should be given regarding the category of electronic money.

Additionally, it should be discussed how to regulate global stablecoins, with a specific mandatory treatment.

The Deposit Guarantee Scheme Directive<sup>20</sup> (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?**

In our view, crypto-assets should not be regarded as bank deposits within the meaning of Community law, since these assets have a different risk profile from deposits and could endanger the DGSD.

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.

---

<sup>20</sup> Deposit Guarantee Schemes Directive (2014/49/EU)

### 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<sup>21</sup> (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".**

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

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

<sup>21</sup> 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)

It is clear that ICOs and the underlying crypto-assets have benefits.

- Traditional IPOs regulation generally imply burdensome, costly and time-consuming processes which are not suited to limited volumes' fund raisings. This is particularly true regarding SMEs looking to raise funds.
- ICOs are an alternative to traditional fund-raising methods with :
  - A more affordable fundraising for start-ups/SMEs: ICOs are faster to implement when compared to other public offerings. Indeed, ICOs could provide a useful alternative funding source for SMEs that would find it difficult or costly to raise capital through traditional funding channels. Issuers can raise capital more quickly with an ICO compared to traditional fundraising methods with less regulatory oversight than IPO for example. ICOs also imply lower costs than those of conventional methods such as marketing, regulatory or settlement costs.
  - An earlier Access to Capital: ICOs were launched by companies at very early stages of development. In this regard it may be considered as a substitute to venture capital funding.
  - No debt or equity in an ICO: ICOs allow start-up firms to raise money without selling equity or taking out debt (e.g. incurring debt burdens the company to repay the debt and make interest payments).
  - Diversification of the investor base / Inclusiveness aspect of ICO: ICOs are also a way to raise money from a diverse investor base as they offer the possibility to tap a global market.
  - Enhanced security, traceability of transactions: from a technical point of view, crypto-assets are cryptographically secured and benefit from characteristics of DLTs (i.e. immutability, permanence, transparency and security). The use of smart contracts may also reduce counterparty risk as the programming of such applications guarantees the automatic execution of a transaction.

These benefits have been presented in an economy analysis published by the AMF in November 2018: <https://www.amf-france.org/en/news-publications/publications/reports-research-and-analysis/french-icos-new-method-financing>

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<sup>22</sup>. 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<sup>23</sup>. 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<sup>24</sup>, 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".**

---

<sup>22</sup> ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019

<sup>23</sup> For example when established market participants operate on private permission-based DLT, this could create entry barriers.

<sup>24</sup> FSB Chair's letter to G20 Finance Ministers and Central Bank Governors, Financial Stability Board, 2018

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

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

The above table has been completed taking into account the fact that there is no global stablecoin at this stage. 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 ("global stablecoins"). In such a global use, the risks regarding financial stability, monetary sovereignty and monetary policy transmissions, and competition would be radically heightened and the risk would thus have been assessed at 5 in the table.

Without this global use, numerous risks exist.

For example, based on IOSCO analysis regarding ICOs (IOSCO, 2018), in the absence of any regulatory framework and supervision, the following risks can be mentioned: the lack of transparency of most ICOs (e.g. the absence of disclosure requirements exacerbating information asymmetries, the lack of any formal auditing process and appropriate due diligence by financial professionals, the lack of information on how the ICO is structured which can give rise to conflicts of interest, etc.), the absence of lock-up period requirements (giving rise to a risk of pump and dump schemes) or the high risk of fraud (e.g. AML/CFT issues, Ponzi scheme, etc.), the unregulated nature of secondary markets. Similarly, many intermediaries have emerged in the ecosystem of crypto-assets offering services such as trading, exchange, custody, portfolio management, in a totally unregulated manner. The customers of these intermediaries are today exposed to numerous risks (cyber risks, market abuse risks, operational risks, risks of asset losses, money laundering risks, liquidity risks etc.). Many risks are also to be dealt with regarding crypto-assets in a broad sense.

"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'*<sup>25</sup> 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

---

<sup>25</sup> G7 Working group on 'Stablecoins', [Report on 'Investigating the impact of global stablecoins'](#), October 2019

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

Stablecoins, because of their relatively stable value denominated compared to other types of crypto-assets, could be widely used as a means of payment. They could facilitate cross-border payments and increase financial inclusion, in particular if they manage to have a global reach. These initiatives highlight certain shortcomings in payment systems, particularly with regard to cross-border payments, which can be costly and slow.

Moreover, stablecoins can be used on a DLT to support interbank settlement and delivery vs payment. Stablecoins could be useful to simultaneously carry out delivery and payment operations on a blockchain. As a result, stablecoins have the potential to significantly increase the efficiency of our market infrastructures and potentially reduce the fragmentation of European industry in this area.

**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".**

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

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

Again, 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, GSCs 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 cryptocurrencies), particularly for emerging countries already suffering from partial dollarization 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. GSCs 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 are amplified in the case of global stablecoins. This may lead to providers (when they are 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) should not be 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 in order to have a sustainable, safe and sound crypto-asset ecosystem in the EU. The AMF is 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.

This choice has been made at the AMF level, based on the following reasons:

- it clearly appeared to be the favored option of the respondents to the AMF's ICO consultation;
- existing framework seemed to a large extent ill-adapted to the structure of the environment (mainly composed of start-ups and lacking market infrastructures);
- the traditional regulation was perceived as too heavy and likely to drive the projects away from France, where they would still be able to offer services to French investors due to the cross-border nature of ICOs. Therefore, if the scope of traditional regulation had been extended to all types of crypto-assets, there would have been a strong risk of flight of innovation, while not ensuring appropriate investor protection;
- the existing framework does not bring all the appropriate safeguards: disintermediated nature of ICOs raises challenges that are not tackled by existing frameworks (legal personality of the issuer, cross-border issuer, AML-CFT for an issuer, security in smart contracts);
- a bespoke and optional regime allowed to have a flexible, proportionate and progressive approach;
- it helped to create a transition phase during which interactions between the crypto-asset environment and the traditional financial sector could be better handled.

In our view, this bespoke regime should be partially based on mandatory requirements (e.g. AML-CFT and fit and proper rules), while other requirements could be optional as it was done in France. Additionally, this common regime should ensure that there is a level playing field in the European Union, avoiding the emergence of various and very different regulatory regimes. A passporting regime between the EU Member States could be introduced. Particular attention should be paid to entities established outside the EU and offering services in the EU. While it is not a question of prohibiting reverse solicitation, it seems essential to subject entities marketing products in the EU to the rules of the European regime. To ensure their proper supervision, they should also have a permanent establishment in the EU.

Again, a specific treatment of global stablecoins should be done with a mandatory regime.

**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.**

➤ **Regarding the PACTE regime (2019)**

The French Law No. 2019-486 of 22 May 2019 (called "PACTE law") has introduced in France a bespoke regime for crypto-assets (optional and partially compulsory) structured around two main axis: an optional visa regime for Initial Coin Offerings and an optional and compulsory regime for Digital Asset Service Providers.

The underlying assets are defined as 'digital assets', with 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).

**1. An optional visa regime for Initial Coin Offerings ("ICOs")**

The PACTE law provides for an optional visa for ICOs' issuers (French or foreign) established in France on a voluntary basis. Issuers who have chosen the visa will be expected to give full disclosure to the AMF (see details in question 21 below), allowing investors to make informed decisions about the ICO. These measures must provide accurate, clear and non-misleading content that helps to understand the risks associated with the offer.



When issuing an optional visa for a public offer of crypto-assets, the AMF shall ensure that the issuer and the offer 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 and Instruction DOC-2019-06. 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 the risks relating to the offering. The information that it contains shall be accurate, clear and not misleading;
- The issuer shall have implemented a mechanism to monitor and safeguard the funds raised in order to guarantee the proper allocation of funds to the planned project;
- 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).

## **2. An optional and compulsory regime for Digital Asset Service Providers (“DASPs”)**

The PACTE law also provides for a bespoke framework governing the activities of secondary market crypto-assets intermediaries called digital asset service providers (“DASPs”). In the same way as with the primary market ICO framework, the PACTE law sets up an optional license for DASPs which are licensed and placed under the supervision of the AMF. However, registration is mandatory for two activities. If an intermediary provides for (1) digital asset custody services and/or (2) buying or selling digital assets for legal tender services in France, this intermediary will have to be register with the AMF, with the Autorité de Contrôle Prudentiel et de Résolution (ACPR)’s assent, before starting its activity.

### **→ A compulsory regime for 2 crypto-assets’ activities**

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).

The registration procedure is mandatory. The AMF will check that the entity complies with the regulations on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT). The assent of the ACPR is required. For these entities, the AMF and the ACPR will verify the following:

- 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):

➔ **An optional license procedure going beyond AML-CFT**

The optional license covers a wide range of activities.

- Services on behalf of third parties:
  - custody of digital assets, meaning in practice the custody of cryptographic keys on behalf of a client;
  - the service of buying or selling digital assets for legal tender;
  - the service of trading digital assets for other digital assets;
  - the reception and transmission of orders for digital assets, meaning the act of receiving and transmitting buy or sell orders for digital assets on behalf of a client;
  - the management of digital asset portfolios, meaning the act of managing, on a discretionary, client-by-client, basis, portfolios that include one or more digital assets under a mandate given by a client;
  - advice to investors in digital assets. This means giving personalised recommendations to a third party, either at their request or on the initiative of the service provider providing the advice, concerning one or more digital assets;
  - digital asset underwriting, meaning the act of purchasing digital assets directly from a digital asset issuer, with a view to subsequently selling them;
  - the guaranteed investment of digital assets, which consists in searching for buyers on behalf of a digital asset issuer and guaranteeing them a minimum amount of purchases by undertaking to buy any digital assets that are not placed;
  - the unsecured investment of digital assets, meaning the act of searching for buyers on behalf of a digital asset issuer without guaranteeing them an amount of purchases.
- The operation of a trading platform for digital assets. 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.

This license remains optional. If an intermediary established in France provides for one or more digital asset services, it may apply for a license provided by the AMF. In this case, the entity must comply with certain requirements in terms of organisation, business conduct and financial resources. The entity will also have to abide by AML-CFT rules if it is not already covered by the mandatory registration (which is only applicable to providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers).

The AMF will publish a list of approved DASPs on its website.

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,...).

For more information on the French regime of digital asset service providers click [here](#)

### **3. A possibility for certain professional funds to invest in digital assets**

Further, the PACTE law modified some rules applying to alternative investment funds ("AIFs") enabling:

- Professional specialised investment funds (provided that they comply with the liquidity and valuation rules applicable to them); and
- Professional private equity investment funds (subject to a limit of 20% of their assets) to invest in digital assets (e.g. such as bitcoins or ethers).

#### 4. Additional measures to better protect investors

Finally, the PACTE law consolidates the AMF's powers in order to provide better protection to investors. The AMF oversees the ICOs that have received its visa and supervises licensed service providers. In the event of non-compliance with the rules, the AMF may hand down sanctions against issuers and providers.

The AMF may publish a "blacklist" of ICOs and DASPs who do not comply with the regulations and may block access to fraudulent websites offering services in digital assets.

Additionally, direct marketing is banned, except for entities being registered, licensed or ICOs having received a visa.

Finally, a review clause is foreseen by 2021 with the aim of evaluating possible changes and necessary adjustments. The PACTE law is considered by the French legislator as a first answer of regulation.

#### ➤ **Regarding the French "Blockchain Order" (2017)**

- Regarding non-listed security tokens on a trading venue within the meaning of MiFID

The French Blockchain Order of 2017 already allows them to be issued and transmitted on the blockchain. However, the scope of the securities in question is limited to units and shares in CIU not admitted to the operations of a central depository, and negotiable debt instruments and shares and bonds not traded on a platform within the meaning of MiFID.

The scope of the Blockchain Order has been intentionally limited to financial securities which are not subject to the European legislation (CSDR). This scope is limited to financial securities which are not admitted to the operations of a central securities depository, i.e.<sup>26</sup> mainly securities which are in registered form. In practice, this means:

- equity securities and debt securities issued by joint-stock companies not traded on a trading venue within the meaning of MiFID II;<sup>27</sup>
- units or shares in collective investment undertakings not admitted to the operations of a central depository;
- negotiable debt securities.

The ledger of holders 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

---

<sup>26</sup> Articles L. 211-7 para. 1 and R. 211-2 of the Monetary and Financial Code.

<sup>27</sup> Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments, amending Directive 2002/92/EC and Directive 2011/61/EU (revision).

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.

**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)**

Crypto-assets that do not fall within the definition of transferable securities as defined by MiFID II are largely in a legal vacuum at the European and international level. A new regulation at EU level for these assets, provided that it is designed in a flexible, proportionate manner and takes duly into account the specificities of the blockchain environment, could definitely serve the objectives of bringing investor protection (by providing reliable information to potential investors), addressing the AML-CFT risks and reducing legal uncertainty for the serious projects being developed in this area.

We believe that a regulatory framework for crypto-assets should harmonise AML-CFT and fit and proper practices at European level, taking duly into account the specificities of the Blockchain environment. One example of the challenge of putting proportionate rules in place is the “travel rule” whose requirements seem to be ill-adapted to the specificities of the blockchain at this stage.

A regulatory framework for crypto-assets should also propose rules in order to guarantee security to investors. Such rules should cover both primary and secondary markets (requirements would for example include minimum levels of own funds, internal control policies and processes for managing effectively IT systems and conflict of interests). Indeed, a regulatory framework based solely on AML-CFT measures would not be sufficient to effectively protect investors and encourage a healthy development of this ecosystem. We believe that it would be necessary to accompany this framework with appropriate measures to regulate primary markets and intermediaries operating in this sector, drawing inspiration from the rules applicable to the regulation of financial services and adapting them to the specificities of digital assets.

**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<sup>28</sup>?**

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

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

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 think that the prudential treatment will have to be specified once we 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 a harmonized application of these possible new rules (i.e. preferably in Level 1 or, at a second best, in Level 2 texts).

---

<sup>28</sup> See the discussion paper of the Basel Committee on Banking Supervision (BCBS) “Designing a prudential treatment for crypto-assets”, December 2019

**Regarding the French digital asset providers regime** (see questions 14 and 15).

In France, licensed DASPs must either have professional indemnity insurance or a minimum amount of equity. This requirement is specified in the AMF instruction describing the content of the application file and the equity requirements for the DASPs.

### **Regarding Investment funds**

As mentioned above (see question 15), the PACTE regime provides for the **possibility for certain professional funds to invest in digital assets**. To that end, the PACTE law modified some rules applying to alternative investment funds (“AIFs”) enabling :

- Professional specialised investment funds (provided that they comply with the liquidity and valuation rules applicable to them); and
- Professional private equity investment funds (subject to a limit of 20% of their assets) to invest in digital assets (e.g. such as bitcoin or ether).

Beyond these aspects, the AMF is traditionally competent with regard to prudential treatment for portfolio asset management companies. We would welcome greater clarity as to the prudential treatment of their exposures to crypto-assets. Such clarity could be brought with:

- a high level principle in level 1;
- rates or threshold in an EU legislation of lower level, so that they can be changed with more flexibility.

### **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?**

As for any type of legislation, the existence of different national regimes may hamper the development of a common European market. In the present case, there is no common approach regarding the legal validity of transfers and tokenisation. In France, a specific order (n°2017-1674) has been adopted in 2017 to authorize the registration and transfer of unlisted securities through the use of blockchain technology. A generalisation and harmonisation of the rules applicable to transfers of unlisted securities at European level would provide legal certainty for investors, but a thorough assessment of the consequences of such an approach should be carried out beforehand. An extension of this mechanism to listed securities could be considered at a second stage in order to encourage STOs, provided that all possible legal obstacles are removed at both national and European levels (see below).

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

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

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

## **Regarding crypto-asset issuance (ICOs)**

See questions 14 and 15 the description of the PACTE law.

The AMF has granted a first approval to an ICO made by French-ICO in December 2019. This first public offering is being made by a company that has developed a platform for fundraising in crypto-assets. The approval is granted until the 1st of June 2020. This ICO is available in the list of offerings that have received the Authority approval.

A dozen other application files for ICO visa approval is currently being reviewed by the AMF's Corporate Finance and Corporate Accounting department. In addition to those files, a dozen of other expressions of interest have been received by the AMF. These concern various type of projects from asset management in the field of renewable energy to distributed applications running on the blockchain.

It is important to note that this visa is optional. In other words, ICOs without the AMF's approval are legal, therefore there might be some ICO issuers in France other than those that are in discussion with our staff. However, ICOs that do not have this optional visa are prohibited from solicitation, patronage and sponsorship activities.

## **Regarding digital asset service providers (DASPs)**

The PACTE Law has also introduced in France an optional and compulsory regime for digital asset service providers. Please refer to detailed description of digital asset services at questions 14 and 15 above.

Please note that the PACTE law does not cover emerging activities such as staking, mining, or crypto-assets lending and repurchasing. We believe it might be too early to regulate these activities as they still are at an early stage of development.

In addition, we draw a distinction between (i) custodial wallet providers (holding the private cryptographic keys on behalf of their clients, and as a consequence having the control over the crypto-assets on behalf of the clients) and (ii) non-custodial wallet providers (providing solutions helping the clients to hold their own private cryptographic keys). Indeed, in the first case, the owner is not responsible for the technical custody of the assets, instead the custodial wallet provider is (and is regulated as such under the PACTE regime). Whereas, in the second case (non-custodial wallet case), the owner is responsible for his own crypto-asset custody and does therefore a "self-custody" of his crypto-assets. Non-custodial wallet providers offer a purely technical solution and do not fall within the scope of the PACTE regime. This approach is consistent with the 5AMLD.

Although the PACTE law came into force in May 2019 the Implementing regulation regarding the DASP regime was published in December 2019. In the meantime, the AMF has received several dozens of expressions of interest with regard to the compulsory registration regime for (i) custody of crypto-assets and (ii) the service of buying or selling crypto-assets for legal tender (more than forty to date). Regarding the optional regime, the AMF has received to date more than twenty expression of interest.

The AMF and the ACPR have granted two first approvals to DASPs (Coinhouse and Coinhouse Custody Services) in March 2020. Additionally, to date, a dozen application files have been filed by the AMF's Markets Department and Asset Management Department for the compulsory registration. Among them, a French large bank is planning to launch (i) a primary market solution and advisory for structuring new crypto-assets, (ii) a crypto-assets' secondary market and risk management solutions, (iii) investment management solutions on crypto-assets, (iv) secured token custody meeting banking industry standards, funds services, as well as (v) banking services on crypto-assets in line with KYC, AML, bank account and cash management requirements. In addition, this entity plans to create a "generic security token" based on a new business chain integrating several products such as bonds, CP and structured products. The project is



based on a public blockchain. For this purposes, the bank is applying for licenses to operate digital assets (DASP status) as well as traditional financial licenses for several investment services.

Another example concerns a major French crypto-asset exchange that is applying for (i) the custody of crypto-assets on behalf third party service, for (ii) the service of buying or selling digital assets for legal tender as well as for (iii) the optional advisory service for investors in digital assets.

Final example with a major US crypto-asset trading platform that is applying for the (i) crypto-assets custody service, (ii) the service of buying or selling digital assets for legal tender as well as for (iii) the optional service of management of a crypto-asset trading platforms.

Several other examples of French and foreign actors wishing to benefit from this new regime could be given. This illustrates the need for regulatory clarification with respect to crypto-assets. We can note that all of these players opt-in for several types of services (e.g. custody of crypto-assets and management of a trading platforms; advisory on crypto-asset and service of buying and selling crypto-assets).

For more information on the French regime of digital asset service providers click [here](#).

## **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<sup>29</sup>. 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.

---

<sup>29</sup> Study from the European Parliament on “Cryptocurrencies and Blockchain”, July 2018

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 (see question 14, 15 and 21).

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 substance 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 DASPs and prevent foreign DASPs (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.

**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...).**

The AMF 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 AMF's 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 (see question 14 and 15 above).

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 ensure<sup>5</sup> that all issuers and their offers provide a certain number of minimum guarantees for better investor protection purpose:

1. The issuer of crypto-asset shall be incorporated as a legal entity established or registered in France;
2. 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.

3. The issuer shall have implemented a mechanism during the offering to monitor and safeguard<sup>7</sup> 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.).

4. 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](#).

**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...).** [Insert text box]

We believe that issuer of crypto-assets should be required to provide certain key information when issuing crypto-assets, as it is already the case 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 (see question 14 and 15 above).

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 ensure that all issuers and their offers provide a certain number of minimum guarantees for better investor protection purpose:

1. The issuer of crypto-asset shall be incorporated as a legal entity established or registered in France;
2. 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 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.

3. 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.).

4. 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:
  - o 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);
  - o 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".**

	1	2	3	4	5	No opinion
The Consumer Rights Directive <sup>30</sup>					5	
The E-Commerce Directive <sup>31</sup>					5	
The EU Distance Marketing of Consumer Financial Services Directive <sup>32</sup>					5	
Other (please specify)						

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

Requirements provided for these directives should be taken into account in order to ensure better protection of the investors. Nevertheless, it should be noted that an assessment of these Directives' provisions would be necessary in order to know which requirements are applicable and which are not depending on the functionality attached to crypto-assets.

Indeed, depending on the nature of crypto-assets (possibly in the long term depending on their classification), not all legal provisions present within the Directives mentioned above will necessarily be applicable.

In general, there is a need to clarify the interaction between existing legislation frameworks when applied to crypto-assets ecosystem.

Any future crypto-asset bespoke regime will have to take into account these problems of interaction between regulatory provisions (including MiFID or PSD2) in order to bring more legal clarity.

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

	1	2	3	4	5	No opinion

The managers of the issuer or sponsor should be subject to fitness and probity standards					5	
The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions					5	
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					5	
Other						

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

Yes, we believe that, beyond the incorporation and the disclosure of information on the offer, the issuer should be subject to the above-mentioned requirements (see also the detailed description of requirements to get an ICO visa in France, provided at question 21 above). The obligations listed in the table are highly relevant.

**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).**

	“Stablecoins”		“Global stablecoins”	
	Relevant	Not relevant	Relevant	Not relevant
The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds...)	R		R	
The issuer should contain the creation of “stablecoins” so that it is always lower or equal to the value of the funds of the reserve	R		R	
The assets or funds of the reserve should be segregated from the issuer’s balance sheet	R		R	
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)	R		R	
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)	R		R	
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating	R		R	
Obligation for the assets or funds to be held in custody with credit institutions in the EU	R		R	
Periodic independent auditing of the assets or funds held in the reserve	R		R	
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	R		R	
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically	R		R	



Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer	R		R	
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. In particular, if retail stablecoins are 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<sup>33</sup> 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”.**

---

<sup>33</sup> Trading venues are a regulated market, a multilateral trading facility or an organised trading facility under MiFID II



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

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

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 (see question 15 above), 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-asset 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".**

	1	2	3	4	5	No opinion
Trading platforms should have a physical presence in the EU					5	
Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					5	
Trading platforms should segregate the assets of users from those held on own account					5	
Trading platforms should be subject to rules on conflicts of interest				4		
Trading platforms should be required to keep appropriate records of users' transactions					5	
Trading platforms should have an adequate complaints handling and redress procedures					5	
Trading platforms should be subject to prudential requirements (including capital requirements)					5	
Trading platforms should have adequate rules to ensure fair and orderly trading					5	
Trading platforms should provide access to its services in an undiscriminating way					5	
Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse				4		
Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)				4		
Trading platforms should be responsible for screening crypto-assets against the risk of fraud				4		
Other : precise recording in the Blockchain, fair clearing and settlement, fair treatment of hard forks (see previous answer)					5	

**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).**

We believe those requirements should not depend on the type of crypto-assets traded on the platform. They seem to be relevant for every crypto-asset.

### **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<sup>34</sup>.

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

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

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

When crypto-exchanges (brokers/dealers) also operate as custodial wallet providers, additional risks can be identified, in particular the risk of absence of segregation of assets held on behalf of clients with assets held for own account, the risk of unfairly treated hard fork (see answer to question 27).

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

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

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

<sup>34</sup> Study from the European Parliament on "Cryptocurrencies and Blockchain", July 2018

Exchanges should be subject to rules on conflicts of interest				4	
Exchanges should be required to keep appropriate records of users' transactions					5
Exchanges should have an adequate complaints handling and redress procedures				4	
Exchanges should be subject to prudential requirements (including capital requirements)				4	
Exchanges should be subject to advertising rules to avoid misleading marketing/promotions					5
Exchanges should be subject to reporting requirements (beyond AML/CFT requirements)			3		
Exchanges should be responsible for screening crypto-assets against the risk of fraud				4	
Other : fair treatment of hard forks (see questions above)					5

**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).**

We believe those requirements should not depend on the type of crypto-assets traded on the platform. Most of the platforms offer each type of crypto-assets, and even though some are more likely to appear as investment tokens, it seems appropriate to apply the same rulebook to all crypto-assets. This choice has been made in France.

In France, the DASP regime introduced by the PACTE law provides for an optional license for the service of (i) buying or selling digital assets for legal tender (also subject to a compulsory registration regime, see question 15 above) as well as the service of (ii) trading digital assets for other digital assets.

This concerns digital assets services providers that provide for a service of buying or selling digital assets in a currency that is legal tender or a service of trading digital assets for other digital assets:

1° either by dealing on its own account when executing the client's order;

2° or by sending the client's orders for execution on a trading platform for digital assets.

Such digital asset service provider licensed for the provision of this services shall comply with some obligations, under the conditions and within the limits provided for by the General Regulation of the AMF (for more information click [here](#)) such as:

- They shall establish a non-discriminatory commercial policy;
- They shall publish a firm price of the digital assets or a method for determining the price of digital assets;
- They shall publish the volumes and prices of the transactions that they have executed;
- They shall execute their clients' orders at the prices displayed at the time of their receipt.
- The persons who effectively manage the service and 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;
- The service provider shall provide evidence that it has established an organisation, procedures and internal control system;

- They shall lay down operating rules;
- They shall ensure fair and orderly trading;
- They shall commit their own capital to the platforms that they manage;
- They shall publish the details of the orders and the transactions concluded on their platforms.

As DASPs, they also have to comply with requirements regarding insurance or equity, internal control procedures, and the resilience of the IT system.

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.

Therefore, in our view, any potential European bespoke regime for crypto-asset intermediaries should take into account these kind of key provisions that would apply to buying and/or selling crypto-asset against fiat currencies or other crypto-assets in order to mitigate the risks above mentioned.

#### 4. Provision of custodial wallet services for crypto-assets

Crypto-asset wallets are used to store public and private keys<sup>35</sup> 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<sup>36</sup>. DLT networks generally provide their own wallet functions (e.g. Bitcoin or Ether).

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

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

	1	2	3	4	5	No opinion
No physical presence in the EU					5	
Lack of adequate governance arrangements, including operational resilience and ICT security					5	
Absence or inadequate segregation of assets held on the behalf of clients					5	
Conflicts of interest arising from other activities (trading, exchange)					5	
Absence/inadequate recordkeeping of holdings and transactions made on behalf of users					5	
Absence/inadequate complaints or redress procedures are in place					5	

<sup>35</sup> DLT is built upon a cryptography system that uses pairs of keys: public keys, which are publicly known and essential for identification, and private keys, which are kept secret and are used for authentication and encryption.

<sup>36</sup> There are software/hardware wallets and so-called cold/hot wallets. A software wallet is an application that may be installed locally (on a computer or a smart phone) or run in the cloud. A hardware wallet is a physical device, such as a USB key. Hot wallets are connected to the internet while cold wallets are not.

Bankruptcy of the custodial wallet provider					5	
Inadequate own funds to repay the consumers					5	
Losses of users' crypto-assets/private keys (e.g. through wallet theft or hacking)					5	
The custodial wallet is compromised or fails to provide expected functionality				4		
The custodial wallet provider behaves negligently or fraudulently					5	
No contractual binding terms and provisions with the user who holds the wallet					5	
Other						

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

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

In France, the DASP regime introduced by the PACTE law provides for an optional license for the service of custody of crypto-assets on behalf third parties (which is also subject to a compulsory registration regime, see question 15 above).

The service providers licensed for the provision of this custody service shall comply in particular with the following obligations (for more information see [Title II of Book VII of the AMF General Regulation: Digital asset service providers](#)):

- They shall enter into an agreement with their clients defining their duties and their responsibilities;
- They shall establish a custody policy mentioning some key information regarding custodian obligations such as:
  - Custodians shall do its utmost to record the movements of digital assets taking place on clients' position registers and to control the means of access to the digital assets;
  - It shall ensure that, in the distributed ledger, its clients' digital assets are separated from its own digital assets;
  - It shall record as soon as possible movements following instructions from the client in the register and shall organise its internal procedures in such a way as to ensure that any movement affecting the registration of the digital assets is evidenced by a transaction regularly registered in the client's account;
  - It shall do its utmost to facilitate the exercise of the rights attached to the digital assets. Any event likely to create or modify the client's rights shall be recorded in the client's position register as soon as possible (e.g. In particular, in case of forks of the blockchain).
- They shall ensure the establishment of the necessary means to return as soon as possible the digital assets or an access to the digital assets held on behalf of their clients;
- They shall segregate holdings on behalf of their clients from their own holdings;
- They shall refrain from using the digital assets or the cryptographic keys stored on behalf of their clients, except with the express prior consent of the clients.

Please note that a distinction should be drawn between (i) custodial wallet providers (wallets used by custodians which hold the crypto-assets on behalf of their clients) and (ii) non-custodial wallet providers. In both cases, a person or a company will own the crypto-assets. However, in one case, (i) the owner will not want to be responsible for the technical custody of the assets, instead the custodial wallet provider will and it will have a control and the crypto-assets. Whereas, in (ii) non-custodial wallet case, the owner will



be responsible for his own crypto-asset custody and will therefore “self-custody” his crypto-assets and control them.

Please also note that the French framework covers the custody of crypto-assets or more precisely the custody of the private keys giving access to these crypto-assets.

Therefore, any potential European bespoke regime for crypto-asset intermediaries should take into account these kind of key provisions that would apply to crypto-asset custody services on behalf third parties in order to mitigate the risks above mentioned.

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

	1	2	3	4	5	No opinion
Custodial wallet providers should have a physical presence in the EU					5	
Custodial wallet providers should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)					5	
Custodial wallet providers should segregate the asset of users from those held on own account					5	
Custodial wallet providers should be subject to rules on conflicts of interest					5	
Custodial wallet providers should be required to keep appropriate records of users’ holdings and transactions					5	
Custodial wallet providers should have an adequate complaints handling and redress procedures					5	
Custodial wallet providers should be subject to capital requirements					5	
Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions				4		
Custodial wallet providers should be subject to certain minimum conditions for their contractual relationship with the consumers/investors					5	
Other: Custodial wallet providers should not use the assets of users, except if they have got their prior and written consent						
Fair treatment of hard forks (see questions above)						

**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).**

We believe those requirements should not depend on the type of crypto-assets traded on the platform. They seem to be relevant for every crypto-asset.

**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).**

Yes, there is no reason in principle to prevent an entity from offering these two services, but this entity will then have to abide by the respective frameworks (one for crypto-assets, one for the security tokens). However we would like to stress that a new regime applicable to the custody of securities registered on DLT should be created, building on the core principles of the existing custody regime while taking into account the specificities of the blockchain environment and the new risks that it may pose.

**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?**

## 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"<sup>37</sup>.**

	1	2	3	4	5	No opinion
Reception and transmission of orders in relation to crypto-assets					5	
Execution of orders on crypto-assets on behalf of clients					5	
Crypto-assets portfolio management					5	
Advice on the acquisition of crypto-assets				4	5	
Underwriting of crypto-assets on a firm commitment basis				4		
Placing crypto-assets on a firm commitment basis				4		
Placing crypto-assets without a firm commitment basis				4		
Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)	1	2				
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)			3		5	
Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)				4	5	

<sup>37</sup> 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.

Services provided by developers that are responsible for maintaining/updating the underlying protocol		2				
Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)		2				
Other services						

**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 order to mitigate risks associated with the crypto-asset ecosystem, we believe that certain types of crypto-asset intermediaries should be subject to specific requirements.

That is the reason why the PACTE law providing for a bespoke framework governing the activities of crypto-assets intermediaries 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 (see question 15 above):

- Services on behalf of third parties:
  - custody of digital assets, meaning in practice the custody of cryptographic keys on behalf of a client;
  - the service of buying or selling digital assets for legal tender;
  - the service of trading digital assets for other digital assets;
  - the reception and transmission of orders for digital assets, meaning the act of receiving and transmitting buy or sell orders for digital assets on behalf of a client;
  - the management of digital asset portfolios, meaning the act of managing, on a discretionary, client-by-client basis, portfolios that include one or more digital assets under a mandate given by a client;
  - advice to investors in digital assets. This means giving personalised recommendations to a third party, either at their request or on the initiative of the service provider providing the advice, concerning one or more digital assets;
  - digital asset underwriting, meaning the act of purchasing digital assets directly from a digital asset issuer, with a view to subsequently selling them;
  - the placing of digital assets on a firm commitment basis, which consists in searching for buyers on behalf of a digital asset issuer and guaranteeing them a minimum amount of purchases by undertaking to buy any digital assets that are not placed;
  - the placing of digital assets without a firm commitment basis, meaning the act of searching for buyers on behalf of a digital asset issuer without guaranteeing them an amount of purchases.
- The operation of a trading platform for digital assets. 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.

For potential requirements, see the DASP Regime (further information available [here](#))

The French framework covers all of these activities, although some of them are still underdeveloped (placement) or non-existent to our knowledge (underwriting). Nevertheless, given the speed at which this system is evolving and its increasing financialisation, it cannot be excluded that all of these services will be

offered in the future. In terms of priority, however, the services of buying/selling digital assets against legal tender, management of a trading platform, custody, and portfolio management for third parties seem to have priority.

Please note that the PACTE law does not cover emerging activities such as staking, mining, or crypto-assets lending and repurchasing or other entities mentioned in the table above. We believe it might be too early to regulate these activities as they still are at an early stage in their development.

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)<sup>38</sup>, 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).**

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 participants perceive them as a 'means 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 'means of payment'.

Notwithstanding this background, we acknowledge that some market participants currently use crypto-assets as a 'means of exchange'.

Furthermore, in our view, those tokens are digital assets in the sense of article L. 54-10-2 2° of the Monetary and Financial Code. Thus, they are not subject to the Second Payment Services Directive.

The conservation of those digital assets by a third party and the execution of the 'means of exchange' transactions may indeed bear significant risks 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 those service providers.

---

<sup>38</sup> Payment Services Directive 2 (2015/2366/EU)

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.

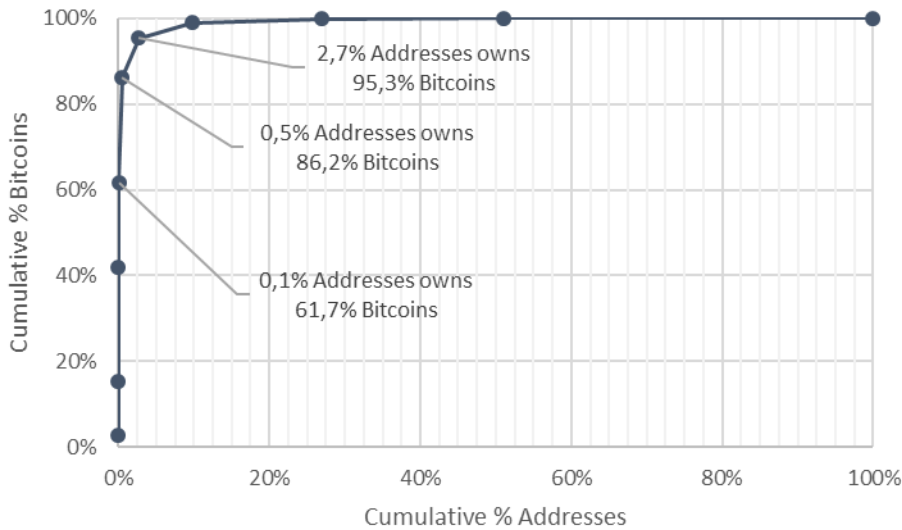
**37) In your opinion, what are the biggest market integrity risks related to the trading of crypto-assets? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".**

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

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

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 own 95% of the bitcoin market and 0,06% of the IP addresses owns 62% of the bitcoin 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 mln of average daily bitcoin volume (about \$6 billion) would be effective transactions.

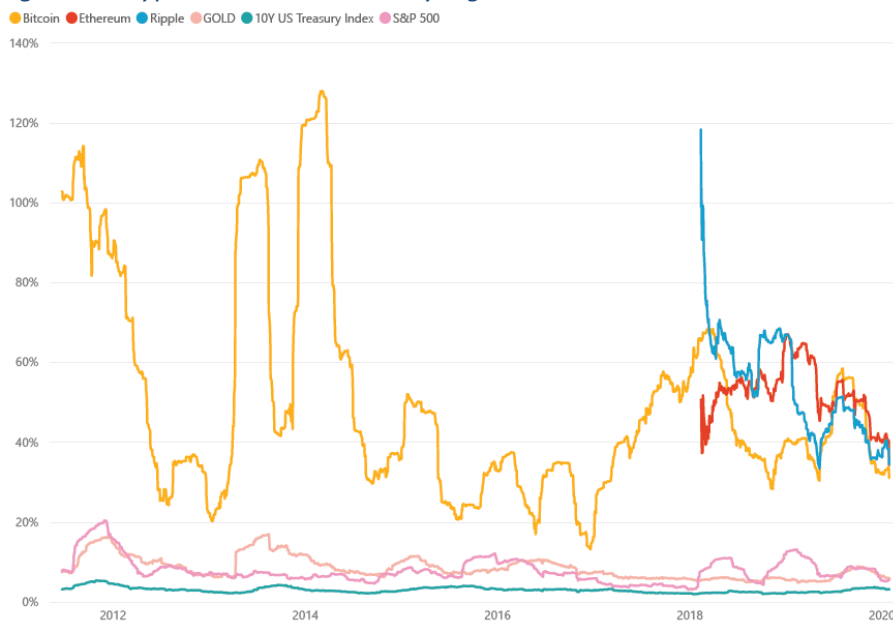
Figure 1 : High level of market concentration



Source : bitinfocharts

The level of concentration of the bitcoin market is stable over time. This eases the price and volume manipulations, which is a major 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



Source : Bloomberg

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 in 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 full extension of the Market Abuse Regulation (MAR) requirements to the crypto-asset ecosystem could unduly restrict the development of this sector. The level of maturity of this environment would need to be taken into account.

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?**

As market abuse risks are relatively high, a regulation on this topic should be introduced. However, it should be common to the EU members, under the supervision of national authorities.

Even if it was created at EU level such regulation should concentrate on major risks and be proportionate in order not to restrict the development of crypto-assets.

As suggested by our answer to the previous question, the EU framework should first state provisions on market manipulation. Those provisions could be very close to the provisions of Article 12 of the Market Abuse Regulation (more precisely 12.1 a, b and c). Of course, there would be a need to adapt the behaviors which shall be given as examples of market manipulation (inserted in Article 12.2 of MAR).

On the use of inside information, new provisions could also be closely inspired by the MAR provisions on the definition of inside information, its use and its communication (except in the normal course of business).

However, in order to have a proportionate approach and for the reasons mentioned in our previous answer, we do not see the necessity to create provisions on the obligation for issuers to disseminate inside information answer.

It should not be proportionate either to introduce like in MAR the relatively marginal abuses related to recommendation to use inside information.

In France we introduced provisions on the need for regulated intermediaries to have systems in place to detect market abuse and we think it is an efficient way to prevent and detect them as for classical financial instruments.

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.**

Identification of parties to transactions is the first condition to be able to identify authors of market manipulation and users of inside information. Additionally, such identification is useful to ensure that transactions are compliant with money laundering and terrorist financing.

**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?**

The fact to have a robust regulation against market abuse in the EU would itself be a strong incentive to favour trades in the EU as the fact to have strong actors of crypto-assets in the EU. Classically, the other way that EU provisions should not be circumvented would be that third countries would also have strong provisions against market abuse.

## **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<sup>39</sup>, 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*"<sup>40</sup>. 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.

---

<sup>39</sup> Anti-Money Laundering Directive (Directive 2015/849/EU) as amended by AMLD5 (Directive 2018/843/EU)

<sup>40</sup> FATF Recommendations



**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).**

The definition of ‘*virtual currency*’ provided by the 5<sup>th</sup> 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 would be an appropriate regulatory response to the diversification of crypto-assets. Indeed, the 5<sup>th</sup> AMLD referring to ‘*virtual currency*’ may be interpreted as covering means of payment only. 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 it has been defined in France, consistently with the FATF’s approach, 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. Regarding CBDC, the French definition excludes, as the FATF’s, digital representation of fiat currencies.

It is alternatively possible to make use of the entire 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 covers the variety of existing crypto-assets as it encompasses all characteristics of crypto-assets’ purposes. However, 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

**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?**

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. There is no common approach at this stage and further work should be done to i) monitor whether the FATF’s standards involve a change in the market, with more users going in the peer-to-peer network; ii) clarify how the risks can be mitigated.

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.”<sup>41</sup>*

**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).**

As a matter of principle, these requirements should be transposed at the EU level. 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 level the 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).

However, an extensive work by the AMF, the ACPR and the French Treasury has been launched, to examine the technical feasibility of the so-called travel rule of the FATF standards. A working group has been set at national level with professionals both from the financial sector and from the crypto-assets sector. All converge to conclude that the travel rule cannot be implemented technically today because of the lack of international network, like Swift for the banking sector, on which information on the originator and the beneficiary of the transfer of crypto-assets can be exchanged between VASPs. This question has also been discussed during a supervisors forum of the FATF on January the 9th and all States around the table agreed that there is no technological solution in place yet. FATF hopes that this recommendation will urge the private sector to develop a new technological solution, like the network Swift for the banks. This solution will not be available soon.

Transposing this rule in a EU regulation is necessary in the long run, but it would be premature to transpose this rule in a EU regulation at this stage. Nonetheless, it is necessary that the Commission, alongside the Member states, gives an impetus to the development of European designed technical solutions and standards to implement FATF's R. 16 when it comes to crypto-assets. Relying only on technical solutions developed by Swiss or US actors would be detrimental to the EU technological sovereignty.

**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**

---

<sup>41</sup> FATF Recommendations

relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Directors and senior management of such providers should be subject to fit and proper test from a money laundering point of view, meaning that they should not have any convictions or suspicions on money laundering and related offences					5	
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					5	

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

As an introduction, the 2008 financial crisis, as well as the 2019 Commission’s “report on the assessment of recent alleged money laundering cases involving EU credit institutions” (also known as “Post mortem”), exposed that the weakness in corporate governance has 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 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. Besides, the 2019 Commission post mortem clearly pointed out that the deficiencies of internal procedures and controls were recurrent explanation of ML-TF incidents involving EU credit institutions. In this context, we analyse the ability of service providers 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.

This approach has been adopted at national level. In the French legal framework of the PACTE law, both requirements are requested from Digital Asset Services Providers who are subject to mandatory registration or optional licensing. Directors and senior management are subject to fit and proper test and services providers must demonstrate their ability to comply with AML obligations.

**3. Consumer/investor protection<sup>42</sup>**

---

<sup>42</sup> 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.

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<sup>43</sup>. Offerings of utility tokens, for instance, do not provide for minimum investment amounts nor are they necessarily limited to professional or sophisticated investors. When considering the consumer protection, the functions of the crypto-assets should also be taken into consideration. While some crypto-assets are bought for investment purposes, other are used as a means of payment or for accessing a specific product or service. Beyond the information that is usually provided by crypto-asset issuer or sponsors in their 'white papers', the question arises whether providers of services related to crypto-assets should carry out suitability checks depending on the riskiness of a crypto-asset (e.g. volatility, conversion risks...) relative to a consumer's risk appetite. Other approaches to protect consumers and investors could also include, among others, limits on maximum investable amounts by EU consumers or warnings on the risks posed by crypto-assets.

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

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

**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.

- (1) Ensuring that the information provided to investors is of high quality
- (2) Requiring professionals providing advisory services to obtain from their clients the necessary information concerning their knowledge and experience of trading in digital assets, their financial situation, including their ability to sustain losses, and their investment objectives, including their risk tolerance
- (3) Finally, clear, legible and non-misleading warnings about the risks associated with investing in such assets.

---

<sup>43</sup> ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019

On appropriate information that should be provided by issuers and or sponsors of crypto-asset see questions 15 and 21 above.

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

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

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

The AMF does 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 investments 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 (global stablecoins should be treated specifically as mentioned above).

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’)<sup>44</sup>.

**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**

Yes, we consider that standards in terms of consumer/investor protection should vary depending on whether the crypto-assets are bought in a public sale or in a private sale. In France, choice has been made to consider as ICOs the offers addressed to more than 150 persons. In this case, the offer falls within the scope of the optional visa and the related protective legal framework. Offers of crypto-assets addressed to

---

<sup>44</sup> See Autorité des Marchés Financiers, French ICOs – A New Method of financing, November 2018

fewer than 150 persons, as they are aimed at a very small number of investors, shall not be eligible to the optional visa and the related protective legal framework.

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

**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).**

Yes, the situation is different in our opinion. If the crypto-assets are bought, the standards in terms of consumer/investor protection should be high, whereas if the crypto-assets are given for free, there should not be any protection beyond a limited information about the risks of loss, because there is no risk for the consumer/investor (except if the crypto-assets create a potential obligation on the crypto-asset holder: in this particular case, the consumer/investor's consent should be asked).

The vast majority of crypto-assets that are accessible to EU consumers and investors are currently issued outside the EU<sup>45</sup>. If an EU framework on the issuance and services related to crypto-assets is needed, the question arises on how those crypto-assets issued outside the EU should be treated in regulatory terms.

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

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

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

The proposal in this response is to provide for a partly mandatory (e.g. AML-CFT and fit and proper; additional requirements in case of tokens reaching global scale) and partly optional regime for other provisions. Therefore, cases of prohibition should be limited to cases of non-compliance with the

---

<sup>45</sup> In 2018, for instance, only 10% of the crypto-assets were issued in the EU (mainly, UK, Estonia and Lithuania) – Source: Satis Research.



mandatory provisions. In these cases, commercialization, distribution and sale of crypto-assets not abiding by the future European framework could be restricted or banned.

Particular attention should be paid to entities established outside the EU and offering services in the EU. While it is not a question of prohibiting reverse solicitation, it seems essential to subject entities marketing products in the EU to the rules of the European regime. To ensure their proper supervision, they should also have a permanent establishment in the EU.

Finally, as mentioned earlier, global stablecoins should be regulated as such with a specific regime mostly based on mandatory requirements. As a result, commercialization, distribution and sale of GSC not abiding by the future European framework could be restricted or 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<sup>46</sup>. 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).**

We believe that, considering the cross-border nature of the crypto-asset environment, the crypto-assets service providers included in Section III. B should ultimately be subject to supervision by the European Authorities. This will ensure a high level of investor protection and eliminate the risk of divergence of interpretation between jurisdictions, while at the same time making the process considerably easier for

---

<sup>46</sup> <https://www.ecb.europa.eu/paym/pol/html/index.en.html>

market participants. In addition, supervision at the European level would allow for better coordination between European countries, ensure harmonisation of rules and facilitate the sharing of information. An analysis will have to be carried out to determine how to achieve this objective in view of the existence of national regimes.

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

New regulatory tools should be designed to serve the dual purpose of fostering the emergence of new players by lowering the cost of entry associated with heavy regulatory requirements, and encouraging European players to leverage on opportunities offered by innovation.

Each of these two objectives involves different tools:

- The emergence of start-ups can be promoted by introducing greater proportionality into our regulatory framework; the ESA review has strongly highlighted the need to introduce more proportionality in our Level 2 and Level 3 Rulebook; ESMA will implement it in its perimeter of responsibility. Another avenue to explore would be to allow phased-in licensing process where one could imagine that a company wishing to test a regulated service with a limited circle of investors and involving small amounts of money could do so without being licensed, subject to compliance with the main principles of regulation (typically those defined in level 1). One possible way to materialize this would be to allow the competent authorities to send no-action letters to the company that would benefit from this scheme, specifying the terms of the projects, the conditions under which the test phase would be authorised (duration, number of participants involved, etc.), similar to the no-action letters used by the SEC in the United States
- The ability of our players to innovate can be encouraged by creating a “digital lab” on a European scale. These will introduce the possibility to lift certain requirements imposed by the European regulations and identified as incompatible, provided that the entity benefiting from this exemption complies with the key principles of the regulations and is subject to enhanced monitoring. An articulation between European and national authorities is required to ensure a level playing field in the experimentations.

Such a mechanism and tools seem essential in the context of experiments related to the use of DLTs in the field of financial services.

In addition, NCAs need to increase their competence as financial regulators on technological issues. One possibility would be to encourage the collaboration of NCAs with European and national competent authorities in this field. 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<sup>47</sup> 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<sup>48</sup>, 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<sup>49</sup> 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)<sup>50</sup> 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,

---

<sup>47</sup> Trading venues are a regulated market, a multilateral trading facility or an organised trading facility

<sup>48</sup> European Markets Infrastructure Regulation (648/2012/EU)

<sup>49</sup> ESMA, [‘Advice on Initial Coin Offerings and Crypto-Assets’](#), January 2019

<sup>50</sup> 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.

there is evidence of only a few instances of security tokens issuance<sup>51</sup>, with none of them having been admitted to trading or traded on a trading venue nor admitted in a CSD book-entry system<sup>52</sup>.

Based on the limited evidence available at supervisory and regulatory level, it appears that existing requirements in the trading and post-trade area would largely be able to accommodate activities related to security tokens via permissioned networks and centralised platforms<sup>53</sup>. 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<sup>54</sup> 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<sup>55</sup> 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.

---

<sup>51</sup> For example the German Fundament STO which received the authorisation from Bafin in July 2019

<sup>52</sup> See section IV.2.5 for further information

<sup>53</sup> 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.

<sup>54</sup> 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.

<sup>55</sup> 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.

**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 in the phenomenon of Security Token Offerings (STOs).

Among these projects, the FORGE project (see question 55 below) 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 token projects have been presented to the Fintech, Innovation and Competitiveness department of the AMF.

The project holders that we have met can be divided into two categories:

- players in the crypto-asset universe who plan to perform an STO instead of or in addition to their ICO: either because they were disappointed by their ICO and are planning an STO to raise additional funds, or because they want to tokenise their shares to give them greater liquidity and thus attract conventional investors (venture capital funds, business angels, family offices). Further, some of these actors plan to expand their intermediary services to security tokens (e.g. custody of digital assets on behalf of third parties, trading platform of crypto-assets, purchase or sale of digital assets, etc.). In France and abroad, several projects for the creation of security token trading platforms have been identified.
- Institutional players willing to integrate the blockchain technology into their infrastructures, and with the purpose of tokenising securities. Some incumbent players are exploring security token offerings and activities in order to assess the feasibility of this type of operation and the related benefits (e.g. including large banks).

The AMF has met several project holders (start-ups and incumbent players) wishing to launch a security token-related business. Among them:

- (i) a major French bank which aims to develop a new offer for the group's clients around four aspects (i) a security token issuance service (assistance to companies for organisation, issuance and placement), (ii) the management of a secondary market, theoretically of the brokerage type, (iii) an asset custody service, and (iv) in the longer run an asset management service proposing the products of investment management companies. It is also planned that additional banking services would be provided to allow transfers between cash accounts and accounts in crypto-assets;

- (ii) A project that aims to establish a blockchain architecture that can be used to perform settlement and delivery of the tokenised financial instruments of SMEs. Another company willing to launch a blockchain based pan-European platform for investment in UCITS units and recordkeeping compatible with all type of distribution channels
- (iii) Several exchanges and trading platforms of security tokens and crypto-asset derivatives as well as tokenised services for financial instrument services.
- (iv) Some other companies planning to develop a platform for trading unlisted securities and fund units enabling investors to exchange these securities over the counter (such companies would ensure matching of supply and demand and management of the order book).

Due to several requests for clarification regarding the possibility to develop a secondary market for security tokens, the AMF published a legal analysis with the view to determine how far it was possible to tokenize financial instruments under the current legal framework. In other words, what are the legal obstacles to the tokenization of financial instruments.

The full legal analysis is available here: <https://www.amf-france.org/en/news-publications/news-releases/amf-news-releases/amf-publishes-depth-legal-analysis-application-financial-regulations-security-tokens>

A challenge ahead is the possibility to use DLT to make payments, especially for DvP. Nevertheless, we are quite optimistic on the capacity of those actors to manage to overcome those issues and accomplish the transfer order of a security token against a coin in DvP in a near future. Indeed, more and more actors intend to tackle the cash leg of securities settlement through the issuance of settlement coins in order to ensure the simultaneous delivery and settlement of tokenized assets.

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

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

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

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 contracts 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 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 simultaneous corruption of all nodes on such distributed infrastructure becomes 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?**

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

**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.**

Yes, it is likely that DLT will significantly impact the role and operation of trading venues and post-trade financial market infrastructures in the future.

DLTs could bring a number of benefits to securities markets, especially more efficient post-trade processes (see question 55). DLT could indeed increase the speed and efficiency of post-trade processes, in particular the clearing and settlement of financial transactions. By increasing the efficiency of back-office infrastructures, DLTs could facilitate trading in a much broader range of financial instruments. The automation enabled by smart contracts would also simplify the trading of structured financial products.

Nevertheless, at this stage, it seems difficult to imagine the extent of the changes given the limited number and scope of practical applications.

So far, to our knowledge, there is no official trading platform listing security tokens in Europe. In the United States, the Open Finance Network platform apparently lists security tokens on the basis of its authorisation as a broker-dealer. It is therefore difficult to imagine what would be the form taken by security token trading in a secondary market.

- **Impact on trading**

If security tokens were to be traded on a platform like today's other forms of existing tokens, a distinction could be made between three types of platforms (see question 66 below):

- **Peer-to-peer or OTC exchange platforms:** these trading venues allow two parties having opposite interests to enter into a relationship, bilaterally agree on a price, and use the blockchain to conclude their transaction. Such trading platforms are close to bulletin boards trading platforms infrastructures (see question 54);
- Platforms built on a **brokerage model** implying own-account intermediation like in the Anglo-Saxon broker-dealer model;
- Platforms whose operation is **similar to that of a multilateral system** within the meaning of MiFID II (order book, absence of discretion, execution of transactions). These platforms can themselves be classified in three categories:
  - **Centralised:** The entire transaction process takes place outside the blockchain (off-chain): trading (establishing a relationship between buying and selling interests), execution of transactions and custody of security tokens, only settlement and delivery being performed on the blockchain which acts as a security recording ledger. This recording on the blockchain takes place when the investor leaves the platform, and not at each transaction;
  - **Decentralised:** The entire transaction process takes place on the blockchain (trading, execution and settlement/delivery) via the use of smart contracts. There is no custody of security tokens by the platform. Unlike the centralised platforms, transaction management is not entrusted to a central operator but to the members of the blockchain network called "nodes";
  - **Hybrid or semi-centralised:** These are all the platforms having a mixed model borrowing from the previous two models depending on the various procedures for trading, transaction execution, security token custody and settlement/delivery. Some platforms have a centralised manager and

others not. This is a hotchpotch category, and the application of the Regulation to these platforms requires analysis on a case-by-case basis.

- **Impact on post-trade financial market infrastructures (CCPs, CSDs)**

One of the most important impacts of DLT in the financial field is certainly that on post-trade financial market infrastructures. Their role needs to be revisited insofar as DLT technologies offer guarantees that reduce the risks that these intermediaries are supposed to address, however other risks may emerge that may deserve to be addressed by regulation.

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

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

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

We agree that a gradual regulatory approach concerning security tokens is necessary.

However, as regards the second part of the question, we do not think it is desirable to favour the use of one form of blockchain over another on the grounds that they are more easily compatible with the existing regulatory framework. The AMF's experience at this stage indicates that there are both serious projects involving open and decentralised blockchains and others based on a closed blockchain approach. Experimentations should be possible with the boundaries of a Digital lab, before considering if necessary a restriction to specific technologies.

**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)<sup>56</sup> and a regulation (MiFIR)<sup>57</sup> 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

---

<sup>56</sup> [Market in Financial Instruments Directive](#) (2014/65/EU)

<sup>57</sup> Markets in Financial Instruments Regulation (600/2014/EU)

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<sup>58</sup> 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?

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

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

Under the French law, it is considered that utility tokens granting access to a service that has not been developed yet do not qualify as securities. However, other Member States (such as Spain for example) draw the same analysis as the SEC and consider that a token shall qualify as a security if the token holder can make a profit based on the issuer's revenues. In other words, not all Member States share the same definition of a security, which means that the applicability of EU legislation to a crypto-asset would vary among member states, leading to a fragmentation of the EU market. For instance, a utility token could be

---

<sup>58</sup> ESMA, '[Advice on Initial Coin Offerings and Crypto-Assets](#)', January 2019

treated as a security in some Member States and a crypto-asset issuer may be subject to the establishment of a prospectus in some Member States and not in others.

It is therefore essential to clarify the border between a security and a crypto-asset: if not, a EU framework for markets in crypto-assets would be inefficient.

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

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

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

It is essential to harmonize the definition of a financial instrument if not, a EU framework for markets in crypto-assets would be inefficient. A definition of a security token at EU level does not seem relevant since a security token already qualifies as a security which has its own definition. Having two separate definitions for a unique instrument does not appear to be a solution.

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

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

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

Where a token displays investment-type features combined with other features, such as utility-type or payment-type characteristics, we believe a case-by-case analysis should be followed. In order to qualify as a security, a token needs to gather several characteristics – among other investment-type features – but it does not mean that if a token displays some investment-type features, it necessarily qualifies as a security. For example, a token that grants a voting right in the issuer’s project (consultative right on a new strategy

for example) would not necessarily be qualified as equity. The same would apply for a token that grants an economic right that does not qualify as dividend (discounts on a service or a product for example).

In order to harmonize the assessment (security token vs. crypto-asset) at the EU level, some guidelines from the European Commission would be necessary.

## 1.2. Investment firms

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

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

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

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

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?

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

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

EU regulation applicable to financial instruments is technology-neutral and should apply entirely in a DLT environment. However, this EU legal framework has not been designed for such environment and is far from being compatible with the objectives that the blockchain industry tries to achieve (disintermediation for example). Some impediments will be developed throughout this consultation paper.

### 1.3. Investment services and activities

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

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

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

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

We believe that the list of investment services is rather appropriate for security tokens, as the latter play the same functions as traditional financial instruments and consequently require the provision of similar services. However, we understand that custody solutions are being developed for security tokens for which no license is required for the sole provision of the safekeeping and administration of financial instruments for the account of clients (which is an ancillary service). Due to high risk of loss of crypto-assets (for hacking reasons for example) the custody of crypto-assets should be regulated for investor protection purposes.

#### 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).

No. The provisions in French law constitute a literal transposition of MiFID II and do not provide for any particular issue which would facilitate or prevent the use of DLT for investment services. As mentioned above, financial regulation is technology-neutral; the same applies to French law. It should however be noted that French law has recently authorized the representation of securities in a DLT, for securities which are not admitted to the operations of a central securities depository.

See response 15 for further information on the Blockchain Order

### 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<sup>59</sup>, 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<sup>60</sup>.

**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).**

So far, to our knowledge, there exists no trading platform listing security tokens in Europe. In the United States, the Open Finance Network platform apparently lists security tokens on the basis of its authorisation as a broker-dealer. It is therefore hard to imagine what would be the form taken by security token trading in a secondary market. This could be based on the various ICO token trading procedures for which numerous models of trading platform already exist. Accordingly, if security tokens were to be traded on a platform like these tokens, a distinction could be made between three types of platforms:

- **Peer-to-peer or OTC exchange platforms:** these exchange venues allow two parties having opposite interests to enter into a relationship, bilaterally agree on a price, and use the blockchain to conclude their transaction;
- Platforms built on a **brokerage model** implying own-account intermediation like in the Anglo-Saxon broker-dealer model;
- Platforms whose operation is **similar to that of a multilateral system** within the meaning of MiFID II (order book, absence of discretion, execution of transactions). These platforms can themselves be classified in three categories:
  - ⇒ **Centralised:** The entire transaction process takes place outside the blockchain (off-chain): trading (establishing a relationship between buying and selling interests), execution of transactions and custody of security tokens, only settlement and delivery being performed on the blockchain which acts as a security recording ledger. This recording on the blockchain takes place when the investor leaves the platform, and not at each transaction;
  - ⇒ **Decentralised:** The entire transaction process takes place on the blockchain (trading, execution and settlement/delivery) via the use of smart contracts. There is no custody of security tokens by the platform. Unlike the centralised platforms, transaction

---

<sup>59</sup> ESMA, [‘Advice on Initial Coin Offerings and Crypto-Assets’](#), January 2019

<sup>60</sup> Recital 8 of MiFIR.

management is not entrusted to a central operator but to the members of the blockchain network called "nodes";

- ⇒ **Hybrid or semi-centralised:** These are all the platforms having a mixed model borrowing from the previous two models depending on the various procedures for trading, transaction execution, security token custody and settlement/delivery. Some platforms have a centralised manager and others not. This is a hotchpotch category, and the application of the Regulation to these platforms requires analysis on a case-by-case basis.

The issue is therefore whether, when security tokens are listed on a platform, that platform is subject to specific regulations. If, finally, the platform's activity can be likened to a trading facility within the meaning of MiFID, then, depending on the case, it will have to comply with the MiFID rules applicable to these trading facilities.

### **1. Requirements applicable to platforms of the OTC or brokerage type**

For OTC or brokerage platforms, it is likely that the services provided will be governed by the MiFID regulations as investment services. It could be the third-party order receipt and transmission service or third-party order execution service (for OTC platforms) or the proprietary trading service (for brokerage platforms). This type of platform, although not, in the legal sense, exploiting a trading facility within the meaning of MiFID, will undoubtedly have to apply for an authorisation as investment service provider (ISP) or financial investment adviser (FIA) depending on the investment service that they provide. The regulatory constraints applicable to the services of order receipt and transmission, third-party order execution and proprietary trading are relatively light and would allow security **token platforms to develop with little constraint in the current legislative framework.**

### **2. Classification of token platforms and trading venues within the meaning of MiFID**

MiFID II defines trading venues as "[...] a system or facility in which multiple third-party buying and selling interests in financial instruments are able to interact". The directive adds that these "systems" or "facilities" should be organised "in a way that results in a contract".

- Two concepts can give rise to interpretation in this definition: the concept of **interaction between multiple buying and selling interests** and the concept of resulting in a contract.

It could be considered, as the FCA did in a consultation of December 2015 on the implementation of MiFID II, confirmed in guidance in its handbook, that "Any system that only receives, pools, aggregates and broadcasts indications of interest, bids and offers or prices shall not be considered a multilateral system for the purpose of MiFID II. To illustrate its analysis, the FCA refers the bulletin boards mentioned in Recital 8 of MiFIR which specifies that a platform should not be termed a "multilateral system" when there is no genuine "trade execution or arranging taking place in the system". According to this Recital, this is the case of "bulletin boards used for advertising buying and selling interests, other entities aggregating or pooling potential buying or selling interests, electronic post-trade confirmation services, or portfolio compression". (see Recital 8 of Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments). The FCA adopts an extensive interpretation because it apparently recognises the description of bulletin board for Seedrs, a crowdfunding platform which develops its own secondary market (for more information click [here](#)).

In the same way, the AMF could consider that platforms for security tokens (or conventional financial instruments) which merely show buying and selling interests without any interaction could not be considered as trading venues within the meaning of MiFID and could therefore be exempted from the regulatory obligations relating to such venues. However, they would still not be exempted from all the provisions of MiFID, because their business of establishing relations between investors would probably

oblige them to apply for an authorisation for the supply of another investment service (RTO, third-party order execution), although admittedly less constraining.

➤ **Second, the concept of resulting in a contract could also be subject to interpretation and** open up possibilities for the development of security token platforms.

In particular, it could be considered that, in the case of hybrid platforms, they are not organised "in a way that results in a contract" to the extent that transactions are executed outside the facility on which trading took place. However, a Q&A from ESMA on MiFID II, updated on 2 April 2019, suggests that whenever the trading venue provides for and describes in its rules in a sufficiently detailed manner procedures for the execution of transactions, the platform should be considered a trading venue within the meaning of MiFID.

To conclude, only security token platforms organised in the form of a bulletin board could be considered as not being trading venues within the meaning of MiFID and therefore be exempted from the MiFID requirements regarding venues. As a consequence, this model would be already applicable without any other legal problem. On the other hand, these platforms would undoubtedly be subject to the ISP authorisation for RTO or third-party order execution. A publication on 6 March 2020 by the AMF of this interpretation of the legislation, like that of the FCA, has provided legal security for the operators (Position DOC-2020-02).

### **3. Legal obstacles relating to the trading of security tokens on a trading venue within the meaning of MiFID**

For platforms which are considered as trading venues within the meaning of MiFID, the present requirements of MiFID do not seem incompatible with the trading of security tokens on certain conditions.

#### **➤ Identification of a platform manager**

The manager must be an entity which has a legal personality. While it is possible to identify a manager for centralised platforms that is impossible for hybrid and decentralised platforms which rely on a public blockchain for the execution of transactions. There is no blockchain manager because of the decentralised nature of the blockchain, which inherently implies no legal link or shared responsibility between participants. The absence of a manager also makes it difficult to apply the European Regulation on market abuse.

#### **➤ Intermediation conditions for MTFs**

A transaction on an MTF implies the presence of at least three members having either ISP status or having sufficient respectability and competence, and having reached an admission agreement with the platform. The requirement of intermediation by an ISP would be extremely inappropriate for the crypto-asset universe insofar as clients have access to the platform directly, without going through intermediaries. It could be envisaged for professional users but apparently does not correspond to the current conditions of organisation of the platforms.

#### **➤ Limited scope for OTFs**

In order to overcome the drawbacks of MTF status, a security token platform could decide to apply for OTF status. OTF clients can access the platform directly, on the sole condition that there be at least three active clients. The disadvantage of this status is that it does not allow trading of equities and units or shares in CIUs on the platform, which is probably a major obstacle to the organisation of a security token secondary market. This status would be useful only for trading bond security tokens.

### ➤ **Other rules laid down by MiFID II (best execution, transparency, tick size, etc.)**

These conditions laid down by MiFID seem at first sight reconcilable with the business model of security token platforms. The best execution requirements should not pose any problems different from those encountered by conventional financial instruments, except for obtaining data to determine in what way the offer proposed by the platform is better than that of the competition with regard to clients' interests. The transparency requirements should not pose problems either, since French platforms are likely to be below the transparency thresholds. However, it will not be easy to calculate these thresholds due to the lack of data to calculate the benchmark market in terms of liquidity. The supervision of tick sizes should not apply to security token platforms either if they are below the liquidity thresholds. From a more general standpoint, and in the same way as for conventional financial instruments, these various obligations are of limited interest if most of the liquidity for the securities is located in a third country.

To conclude, the only security token platforms within the meaning of MiFID which could develop without major constraints under the present regulations are centralised platforms based on a public or private blockchain which adopted MTF status (existence of a manager). Clients would obtain access either in an intermediated manner via an ISP or directly provided that they are trading on their own account and that they meet conditions of respectability, competence and sufficient financial resources. The latter possibility would deserve to be brought to the attention of the market participants concerned who are not necessarily aware of it, for example in the form of a publication (Article L. 424-5 of the Monetary and Financial Code).

Centralised platforms in the form of an OTF with direct access for clients could develop legally, but with significant constraints which could call into question their business model. In particular, these platforms could not propose trading in equities (or units or shares in CIUs). They could only allow the trading of bond security tokens, requiring another type of authorisation to be able to trade equities.

At the other end of the chain, on the other hand, the development of security token trading platforms of the hybrid or decentralised type seems impossible in the current state of the law if they are not operated by an identified manager. An adaptation of the financial regulations in the medium term to address the specific requirements of security token trading platforms would be a necessary condition for the development of platforms of the hybrid or decentralised type and platforms based on a public blockchain.

### **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).**

The investment in security tokens poses similar risks for prospective investors than that of traditional financial instruments: liquidity risk, counterparty risk, market risk, etc. do also exist in a DLT environment. As a consequence, similar investor protection rules should benefit investors so that they can make an informed decision in whether they invest in security tokens or not. We thus believe that the current scope of investor protection rules are appropriate for security tokens: the need for a suitability/appropriateness is still important for such securities and information obligations are also necessary for investors to make an informed investment decision.

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

We believe that the legal framework with regard to marketing communication is strong enough to give clients or potential clients fair, clear and not misleading information. The mere fact that security tokens are circulating in a DLT environment is not sufficient to make a case for establishing specific requirements on the marketing of such securities via social media or online. However, emphasis should be placed on investor protection in order to protect client against potential countless scams that are available on the internet. Investment firms and authorities should then play a preventive role for the avoidance of such situations.

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

Legally speaking, we do not see any particular issue in applying MiFID investor protection requirements to security tokens. Investor protection rules are mainly based on information given to clients (inducements, post-sale reporting, costs and charges, best execution, etc.).

Operationally however, investment firms who would apply MiFID 2 investor protection requirements in respect to security tokens would probably raise the same issues that they currently encounter regarding traditional financial instruments (the cost and charges' regime for example).

## **1.6. SME growth markets**

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

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

Yes, DLT has the potential to make the financial sector more efficient. Today's SME Growth Markets operate with the same post-trade infrastructures as trading venues listing larger issuers, which entails significant costs. By reducing transaction costs, DLTs can provide additional liquidity in this market segment, although liquidity depends on several other factors. Furthermore, the use of DLTs enables SMEs to get to know their shareholders and interact with them in a simplified manner.

## **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<sup>61</sup> shall have in place effective systems procedures and arrangements to ensure that members are only permitted to provide such services if they are investment firms authorised under MiFID II or credit institutions. The same requirements also apply to MTFs and OTFs according to Article 18(5). These requirements could be an issue for security tokens, considering that crypto-asset trading platforms typically provide direct access to retail investors.

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

No. We do not believe that putting in place effective systems, procedures and arrangements to ensure that trading venues' trading systems are resilient, have sufficient capacity and are fully tested would pose any particular issue on a legal and operational standpoints.

However, as regard the DEA (direct electronic access) regime, it remains to be seen how the regulatory scope for security tokens will develop as there is no intermediation with regard to the access of a trading venue in the crypto-asset industry. Should the security tokens' market be available to anyone to access, the DEA regime would therefore be irrelevant and inapplicable.

**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).**

We do not believe that there is merit in reinforcing the legislative rules on admission to trading criteria for these assets. Level 1 provides that financial instruments must be capable of being traded in a fair, orderly, and efficient manner, and, for transferable securities, to be freely negotiable, in order to be admitted to trading on a regulated market. Level 2 (Regulation (EU) 2017/568 of the EU Commission) gives some criteria to determine whether a transferable security is capable of being traded in a fair, orderly and efficient manner. We consider that these conditions are sufficient for the purposes of an admission to trading in a regulated market of security tokens. Taking into account the nature of security tokens seen today, they would likely be qualified as a transferable security under MiFID 2. Proposing more criteria to determine

---

<sup>61</sup> 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)



their capacity of being traded in a fair, orderly and efficient manner would undoubtedly create more obstacles to the admission of trading of traditional transferable securities, unless security tokens constitute a new category of financial instrument. In the case of a new sub-category of financial instrument, we do not see which criteria other than those attributed to transferable securities would be relevant for the purposes of the admission to trading to security tokens. The above-mentioned level 2 regulation gives examples of information useful for the assessment of the capacity of transferable securities of being traded in a fair, orderly and efficient manner (e.g. historical financial information, information about the issuer, information providing a business overview). We do not see which additional information could be required, especially in the context of a very nascent market.

We also understand that reinforcing rules on admission to trading for these assets would likely to be an obstacle for a subsequent organization of an efficient secondary market

### **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).**

**We agree** with the fact that trading crypto-assets is available for any person, without any intermediation.

Allowing a direct access to trading venues to anyone, without any MiFID member to perform a suitability or appropriateness test for example, may undoubtedly create investor protection risks. The client would not be owed any information obligation from an intermediary, jeopardizing an appropriate protection. A regulated MiFID intermediary could inform its clients of the traditional risks an investment in a financial instrument poses, potentially deterring them to invest if a financial instrument is not appropriate to their risk profile. Save for any deposit or investment limit imposed by crypto-asset platforms, any client could potentially invest in any security tokens without being certain to make a well-informed investment decision.

Moreover, best execution requirements would neither apply, preventing retail clients to obtain the most advantageous price for the security tokens. Post-trade information would neither be owed to the client (information laid out in article 59 of the delegated regulation (EU) 2017/565).

Another impediment (not MiFID-related) would be the increase of KYC checks of any client of the trading venues, the total number of which would certainly surpass the number of traditional members/clients of trading venues.

One significant benefit of allowing a broader base of clients to access trading venues for security tokens is cost-based: the total amount of the investment would be less important for investors. Indeed, the client would not pay any broker fees, except for the trading venues' fees.

In a more comprehensive way, it seems that the benefits associated to the blockchain derive from the



disintermediation it enables. Imposing intermediaries even though the technology enables direct transactions without them could be considered counterproductive.

### 1.10. Pre and post-transparency requirements

MiFIR<sup>62</sup> 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<sup>63</sup> of security tokens platforms. For the transparency requirements, it could perhaps be more difficult to establish meaningful transparency thresholds according to the calibration specified in MIFID, which is based on EU wide transaction data. However, under current circumstances, it seems difficult to clearly determine the need for any possible adaptations of existing rules due to the lack of actual trading of security tokens.

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

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

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

MiFIR transparency requirements aim to increase transparency on trading opportunities and prices on financial instruments. They also allow for a better price formation of such instruments.

In the context of a very nascent industry, compliance with transparency requirements would allow market participants and competent authorities to have a deeper knowledge of the security tokens' market. Prospective market data would certainly be a useful metric for the purposes of making a well-informed decision.

Furthermore, the use of waivers could be particularly relevant for larger trades that could lead to a negative impact on the price formation.

However, it is too soon to determine whether the transparency regime applies to security tokens because it is mainly conditional upon the fact that they meet the necessary liquidity threshold. Depending on whether they constitute a share or a bond or else, it is less likely that they would be deemed as liquid. The latter will depend on many parameters but the fact that there is no current secondary market for such instruments makes it difficult to assess their liquidity.

---

<sup>62</sup> In its Articles 3 to 11

<sup>63</sup> MiFID II investment firms must take adequate measures to obtain the best possible result when executing the client's orders. This obligation is referred to as the best execution obligation.

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

On a legal standpoint, we do not see any obstacles in complying with the transparency requirements. Crypto-assets platforms often provide for pre-trade transparency with an order-book available for every client to see (post-trade transparency seems not to be available in these platforms but transaction data can be found when viewing the relevant blockchain). Traditional trading venues entering into the security token business should not encounter any difficulty in complying with transparency requirements, which are already obligations that they should abide by for financial instruments.

Operationally speaking, as said before, the market of security tokens is currently too insignificant for the pre and post-trade transparency requirements to apply.

### **1.11. Transaction reporting and obligations to maintain records**

MiFIR<sup>64</sup> 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).**

We do not see any legal obstacle for the purposes of the reporting regime.

## **2. Market Abuse Regulation (MAR)**

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

Security tokens are covered by the MAR framework where they fall within the scope of that regulation, as determined by its Article 2. Broadly speaking, this means that all transactions in security tokens admitted to trading or traded on a trading venue<sup>65</sup> are captured by its provisions,

---

<sup>64</sup> In its Article 25 and 26

<sup>65</sup> Under MiFID Article 4(1)(24) 'trading venue' means a regulated market (RM), a Multilateral Trading Facility (MTF) or an Organised Trading Facility (OTF')

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?**

We think so. It is due to the wideness of Article 7 and 8 of MAR and to the way they are framed, notably by the reference not to the object of inside information but to the fact it is precise, nonpublic and able to sensibly influence the prices. The definition of the use of inside information, by buying or selling, is also very large and adapted. However, as already said in the answer to question 38, it is important to have the specific definition of inside information related to orders from a client which are not yet introduced in the order book (see. MAR 7.1 d).

## **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?**

For now in France crypto-assets which are financial instruments are not negotiated on platforms such as classical financial instruments. This situation may change in the future but for this reason we have no experience of this topic. We can only observe that for the use of inside information the MAR definition of market manipulation has proved very large and adapted.

### **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?**

This risk cannot be completely excluded as some crypto-assets can give access to specific products or services which can themselves be related to instruments covered by MAR or can have underlying assets.

However, this link seems indirect and weak and in a proportionate approach of a new regulation we do not see for now a need to introduce a provision to extend the MAR scope in this case.

### 3. Short Selling Regulation (SSR)

The Short Selling Regulation<sup>66</sup> (SSR) sets down rules that aim to achieve the following objectives: (i) increase transparency of significant net short positions held by investors; (ii) reduce settlement risks and other risks associated with uncovered short sales; (iii) reduce risks to the stability of sovereign debt markets by providing for the temporary suspension of short-selling activities, including taking short positions via sovereign credit default swaps (CDSs), where sovereign debt markets are not functioning properly. The SSR applies to MiFID II financial instruments admitted to trading on a trading venue in the EU, sovereign debt instruments, and derivatives that relate to both categories.

According to ESMA’s advice<sup>67</sup>, 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".**

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

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

Our responses below are made on the basis that the shares or debt instruments that fall within the scope of SSR may be technically and legally issued in a DLT (which is not the case at this stage, since CSDR practically prevents to issue in DLT shares that are admitted to trading on a trading venue (see below)).

Transparency for significant net short positions: We are of the view that the fact that a share is issued in a DLT should not impact the application of transparency obligation pertaining to the holder of net short positions set forth in Article 5 of SSR.

<sup>66</sup> Short Selling Regulation (236/2012/EU)

<sup>67</sup> ESMA, [‘Advice on Initial Coin Offerings and Crypto-Assets’](#), January 2019

Restrictions on uncovered short selling: We are of the view that the fact that a share falling within the scope of SSR is issued in a DLT should not impact the applications of the restrictions on uncovered short selling set forth in Article 12 of SSR.

Competent authorities' power to apply temporary restrictions to short selling: We are of the view that the fact that a share is issued in a DLT should not impact the possibility for competent authorities to apply temporary restrictions to short selling in accordance with Article 23 of SSR.

**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?**

No.

**4. Prospectus Regulation (PR)**

The Prospectus Regulation<sup>68</sup> establishes a harmonised set of rules at EU level about the drawing up, structure and oversight of the prospectus, which is a legal document accompanying an offer of securities to the public and/or an admission to trading on a regulated market. The prospectus describes a company's main line of business, its finances, its shareholding structure and the securities that are being offered and/or admitted to trading on a regulated market. It contains the information an investor needs before making a decision whether to invest in the company's securities.

**4.1. Scope and exemptions**

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

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

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

---

<sup>68</sup> Prospectus Regulation (2017/1129/EU)

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

We consider that the existing regime shall apply to security tokens without different or additional exemptions. The form of a security or the technology used to register it shall not have an impact on the investor's protection

**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<sup>69</sup> 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).**

---

<sup>69</sup> ESMA, [Guidelines on Risks factors under the prospectus regulation](#) (31-62-1293)

The Delegated Regulation should include a specific schedule regarding security tokens.

A full prospectus approach seems to be the best option in order to take into account the specific features of security tokens.

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

There does not seem to be any technical obstacles to obtain an ISIN code for the purpose of issuing a security token. ISIN codes are granted to issuers by Euroclear the national numbering agency, according to the rules of the international Association of National Numbering Agencies.

**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).**

Regarding security token issuance, we believe that the Prospectus Regulation appears compatible with security tokens. Apart from a few practical problems, the legal framework does not prevent the issue of security tokens. However, the information contained in the prospectus will have to be adapted to the specific features of security tokens.

- **The applicability of the Prospectus Regulation with regard to the legal classification of security tokens**

There are still relatively few STO projects and, for European projects, they share the common characteristic of being issued by way of a public offer below certain thresholds which exempt them from the obligation of producing a prospectus, probably because of the legal uncertainty surrounding security tokens (see question above).

- **Specificities resulting from application of the Prospectus Regulation to STOs**

In practice, the question is whether the prospectus schedules defined by the Prospectus Regulation are appropriate for STOs.

The analysis of the different sections of a prospectus highlights certain characteristics resulting from this type of offer. And yet, these characteristics are not specific to security tokens and these questions are generally raised in the same way for conventional financial instruments.

**Definition of the territory in which the offer is made**

As part of the information which should appear in the prospectus concerning the conditions of the offer, the countries in which the public offer is made are specified. Just like for ICOs, **the question of the territory in which the offer is made can be raised for STOs to the extent that the public offer is made to all net surfers once it is accessible on a website.** It therefore seems difficult in practice to limit the potential recipients of the offer.

We note that the issuer Bitbond Finance considered that the public offer concerned Germany only. Moreover, the prospectus states that "any country in which the offer is illegal" is excluded from the scope of the prospectus. Likewise, investors who are US or Canadian residents for tax purposes have been excluded from the offer.



However, we note that insofar as it is possible for anyone to obtain access to the website, it could be appropriate to consider that the public offer extends beyond the borders of Germany. **If it were to be considered that an offer on the internet entailed making a public offer beyond France, then the AMF would have to require a passported prospectus of the issuer and, on behalf of the issuer, send a summary of the prospectus to the authorities of the other relevant Member States.** This problem is not specific to security tokens but to marketing on the internet, and it is posed in the same way for conventional financial instruments.

Information concerning token listing

The Prospectus Regulation requires the issuer to provide information regarding the markets on which the securities will be listed or admitted to trading.<sup>70</sup>

As part of an STO, token listing is problematic. In this respect, the lesson of the prospectus prepared by Bitbond Finance is interesting. This issuer stated that this factor was "not applicable", specifying that the token would not be admitted to trading on a regulated market within the meaning of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 or on any other equivalent market. The issuer also specified that on the date of the prospectus, it did not intend to carry out such an admission of tokens to trading on a regulated market or on any other market, and had no intention of doing so in the future. However, the issuer specifies that it cannot be ruled out that token holders may exchange their tokens directly with other people or that the tokens could be listed at the request of investors or any other person on an unregulated online crypto-asset platform.

**In any case, the issuer should provide information on the token's listing, in accordance with the legal framework applicable to this listing.**

Information on the tax regime relating to withholding tax in the country or countries in which the offer is made

The Prospectus Regulation requires that the issuer provide information on tax treatment. Regarding this, Prospectus Regulation 3 requires that the issuer provide information concerning any withholding tax applicable to income from the securities in question from the viewpoints of both the country in which the issuer has its head office and the country (or countries) in which the offer is made. However, Prospectus Regulation 3 specifies that "the prospectus should still contain appropriate information on taxation where the proposed investment entails a specific tax regime, for instance in the case of investments in securities granting investors a favourable tax treatment."

**Since an STO distributed via the internet is sent to an unspecified group of persons, a description by the issuer of possible favourable tax treatment is likely to be difficult, especially for small companies and start-ups, given the diversity of tax exemption potentially applicable to investors.** Under these conditions, the question may be asked as to whether it would be acceptable for certain information concerning the tax exemptions to be omitted from the prospectus by the issuer. However, the same question arises in the case of public offers of conventional financial securities on the internet, in the same way as for security tokens.

Multiple subscription prices

---

<sup>70</sup> In particular, the Prospectus Regulation invites the issuer to provide "an indication as to whether the securities offered are or will be the object of an application for admission to trading, with a view to their distribution in a regulated market or other equivalent markets with indication of the markets in question" and the New Prospectus Regulation invites the issuer to provide, under the "details of the offer" (point VI of Annex III), information on the "markets".

Offers sent on a blockchain generally propose prices that are differentiated depending on the date on which the investor subscribes to the offer. But Prospectus Regulation 3 requires that the issuer indicate in the prospectus "the price at which the securities are offered". Even though article 17 of Prospectus regulation offers an alternative to the indication of the price in the Prospectus (indication of the maximum price or of the method of valuation), it will have to be clarified whether it is possible to accept an offer made at various prices, provided that this be mentioned in the prospectus, or whether the issuer should be required to provide a single price for a given offer. If this second option were chosen, then the prospectus should present to investors no longer a single offer but a series of several offers.

It may be noted that the STO prospectus approved by the BaFin mentions various prices for the offer.

The absence of an investment service provider as intermediary

At present, investment service providers operate as intermediaries when making an offer of securities to the public. It is they who are responsible for verifying compliance with the obligations regarding anti-money laundering and combating the financing of terrorism on behalf of the issuer at the time of subscribing to the securities.

Within the framework of STOs, if they are organised on the same model as ICOs, it is unlikely that the issuer will use an ISP as intermediary for the subscription. Therefore, **the issuer is not obliged to comply with the same AML/CFT obligations as ISPs, and no check will be made on security token subscribers.** It should be noted that this fact is already applicable to issuers who decide to keep the issued securities ledger themselves. In the case of ICOs, on the contrary, it was chosen to make verification of the AML/CFT requirements by the issuer compulsory.

To conclude, the Prospectus Regulation appears compatible with security tokens. Apart from a few practical problems, the legal framework does not prevent the issue of security tokens. However, the information contained in the prospectus will have to be adapted to the specific features of security tokens.

**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).**

We consider that the existing regime shall apply to security tokens. The form of a security or the technology used to register it shall not have an impact on the investor's protection. Therefore, we believe that there is no reason to apply an *ad hoc* regime to security tokens. However, some adjustments to the margin would be necessary.

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

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

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

The issuer shall provide a description of the main risk factors specific to the project, the tokens and the STO presented in the prospectus document.

The issuer is invited to group these risks according to their type and to the following classification and, where applicable, to describe the measures taken to prevent these risks.

The risks described by the issuer shall include *at least* the following risks:

**1. Economic risks**

- risk of partial or complete loss of the investment;
- currency exchange risk, including to euro or any foreign currency, borne by the subscriber;
- risk related to valuation of the tokens;
- risk of lack of liquidity for the tokens;
- where applicable, risk due to the lack of secondary market.

**2. Technological risks**

- risk of errors or security flaws allowing hacking or theft of the issuer's data;
- risk of loss or theft of the medium storing the subscriber's private key;
- risks related to the asset monitoring and safeguarding system;
- risks related to the distributed ledger technology on which the tokens are registered and the platforms on which the tokens can be exchanged.

**3. Risks related to the project**

- risk of failure at launch or of technical and operational development of the project;
- risk of a substantial change in the project and in the rights attached to the tokens;
- where applicable, risk due to the lack of regular communication by the issuer concerning its project or any event which could have an impact on the project;
- risks due to the lack of visibility concerning the regulations applicable to the token offering in all the jurisdictions in which the tokens will be offered, and the tax treatment applicable to the token subscribers.

**5. Central Securities Depositories Regulation (CSDR)**

CSDR<sup>71</sup> 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

---

<sup>71</sup> Central Securities Depositories Regulation (909/2014/EU)

with an authorised CSD. However, ESMA underlines that there may be some national laws that could pose restrictions to the use of DLT for that purpose.

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

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

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

	1	2	3	4	5	No opinion
definition of 'central securities depository' and whether platforms can be authorised as a CSD operating a securities settlement system which is designated under the SFD				4		
definition of 'securities settlement system' and whether a DLT platform can be qualified as securities settlement system under the SFD			3			
whether records on a DLT platform can be qualified as securities accounts and what can be qualified as credits and debits to such an account;				4		
definition of 'book-entry form' and 'dematerialised form'	1					
definition of settlement (meaning the completion of a securities transaction where it is concluded with the aim of discharging the obligations of the parties to that transaction through the transfer of cash or securities, or both);			3			
what could constitute delivery versus payment in a DLT network, considering that the cash leg is not processed in the network					5	
what entity could qualify as a settlement internaliser			3			
Other						

**Please explain your reasoning.**

**The AMF is of the view that the question whether settlement of crypto-assets representing rights on underlying financial instruments would fall under the definition of a 'system' under the SFD, and the definition of a CSD under the CSDR is fundamental and should be carefully assessed.**

The AMF believes that the settlement and delivery of certain security tokens raises major issues. The settlement of certain securities is governed by the CSDR at European level. Article 3(2) of CSDR requires that securities traded on a trading venue within the meaning of MiFID II be "recorded in book-entry form

in a [central depository] ".<sup>72</sup> The objective sought by the European legislator is "[...] to ensure that all such securities] can be settled in a securities settlement system."<sup>73</sup>

The issue is whether security token trading platforms could be authorised as a central securities depository, managing a securities settlement system. The securities settlement systems covered by the CSDR<sup>74</sup> are those described by the Settlement Finality Directive,<sup>75</sup> i.e. systems which have been reported to the European Commission<sup>76</sup> and which, accordingly, can benefit from rules derogating from insolvency proceedings law in the event of the default of a participant in the system.

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).

The AMF is of the view that the current regulations (CSDR, Settlement Finality Directive, obligations relating to custodians) cannot ensure settlement and delivery entirely on the blockchain. Several legal obstacles can be identified: (i) the need to identify a blockchain manager acting as a securities settlement system, which de facto excludes decentralised security token platforms and, to a certain extent, the use of public blockchains; (ii) the obligation of intermediation by a credit institution or an investment firm so that individuals may obtain access to the settlement and delivery system, which does not seem compatible with the current functioning of crypto-asset platforms by direct access; (iii) recognition of the right of ownership at the level of the custodians and not by the recording of the security tokens in the blockchain; and (iv) the obligation of settlement of securities in cash, in central bank or commercial currency.

The main requirements laid down by the CSDR and the Settlement Finality Directive are as follows.

**Identification of a system manager:** A securities settlement system must have a manager who is the person who applies for the central depository authorisation.<sup>77</sup> 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 permissioned public blockchain (use of the underlying blockchain technology but enacting of specific operating rules by a service provider).

---

<sup>72</sup> Article 3(2) of the CSDR: "Where a transaction in transferable securities takes place on a trading venue the relevant securities shall be recorded in book-entry form in a CSD [...]".

<sup>73</sup> Recital 11 of the CSDR.

<sup>74</sup> Article 2.1 10) of the CSDR.

<sup>75</sup> Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, as amended by Directive 2009/44/EC of the European Parliament and of the Council of 6 May 2009.

<sup>76</sup> In accordance with Article 330-1 of the Monetary and Financial Code which transposes the Settlement Finality Directive, reporting is done to ESMA.

<sup>77</sup> Article L. 330-1 II 5° of the Monetary and Financial Code taken from the Settlement Finality Directive.

**Obligation of intermediation:** The list of persons authorised to take part in a securities settlement system<sup>78</sup> does not include natural persons. But, as mentioned earlier, these facilities are characterised by direct access of clients including private individuals. **This obligation of intermediation is an impediment to the development of all security token platforms insofar as it would require that clients go through an intermediary** (probably credit or investment institutions). In the SFD, it could be considered extending the list of persons authorised to take part in the securities settlement system to include natural persons subject to certain conditions.

**Recording in book-entry form with the central depository:** Article 3(2) of the CSDR requires that securities traded on a venue within the meaning of MiFID be recorded on an account maintained by the central depository, the securities account being defined as being an "account on which securities may be credited or debited".<sup>79</sup> In its January 2019 opinion on ICOs and crypto-assets, ESMA considers that the CSDR is not prescriptive regarding the nature of the recording 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 up to 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.<sup>80</sup>

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. However, routing via the intermediary represented by the CSD remains an obligation. As things stand at present, a platform listing security tokens should therefore perform settlement and delivery either via another market participant authorised as central securities depository or by being itself authorised as central securities depository.

**Custodians:** In the current state of the legislation, recording on an account in the CSD is not equivalent to a deed of ownership. This is obtained only by recording on an account maintained by a custodian.<sup>81</sup> **The legal security of security token owners is not ensured if the securities are issued only on the blockchain. As things stand at present, it would therefore be necessary for security token platforms to go through another intermediary in addition to the CSD – the custodian– who would record the security token transfers in its accounts to reflect their transmission on the blockchain.** In the current framework, the use of a custodian is necessary to ensure the holder's right of ownership of the security. It would therefore be necessary to extend the possibility of registering securities on the blockchain to securities admitted to transactions with a central depository.

---

<sup>78</sup> Article L. 330-1 II 1° to 9° of the Monetary and Financial Code taken from the Settlement Finality Directive.

<sup>79</sup> Article 2.1 (28) of the CSDR.

<sup>80</sup> ESMA opinion of 9 January 2019 on ICOs and crypto-assets: Paragraph 159: "Based on the above, where crypto-assets qualify as transferable securities and are traded on trading venues, their issuer, provided it is established in the Union, shall arrange for such securities to be represented in book-entry form with an authorised CSD as defined under Article 2(1) of the CSDR. Other than the reference to the use of 'securities accounts'<sup>53</sup>, the CSDR does not prescribe any particular method for the initial book-entry form recording, meaning that any technology, including DLT, could virtually be used, provided that the book-entry form is with an authorised CSD. However, there may be national rules that could pose restrictions to the use of DLT for that purpose. The legal nature of a securities account (i.e. statutory record, contractual construct or accounting device) and the legal nature and effects of book entries are still embedded in national law."

<sup>81</sup> Article L. 211-3 of the Monetary and Financial Code



**Central Securities Depository operating rules:** The CSDR imposes numerous operating rules on CSDs (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),<sup>82</sup> supervision, issuance integrity, and protection of securities (asset segregation)<sup>83</sup>. 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 (the settlement discipline and issuance integrity rules could, for example, prove useless). Apart from the costs, these requirements appear inadequate for the way in which the blockchain operates (unfalsifiable distributed ledger, smart contracts).

**Classification of a blockchain as a securities settlement system:** CSDR provides that a CSD is to operate a settlement system for the titles which have been entered on its books. If security tokens could be recorded by book-entry on a blockchain via a CSD, this 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.<sup>84</sup> This definition does not seem incompatible with settlement on a blockchain. French 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 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.

At this stage, the AMF's stance (duly taking into account ESMA's advice published in January 2019 on initial coin offerings and crypto-assets) is that settlement of crypto-assets representing rights on underlying securities / financial instruments in permissioned networks and centralized platforms<sup>85</sup> 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 our opinion is the case despite the absence of definition of 'book entry' and 'dematerialized form')

---

<sup>82</sup> Article 41 of the CSDR.

<sup>83</sup> Article 38 of the CSDR.

<sup>84</sup> Article L. 330-1 of the Monetary and Financial Code: "I. – An interbank settlement system or system used for settlement and delivery of financial instruments consists of a national or international procedure which organises relations between at least three parties, not counting the system manager, defined in 5° of II of this article, nor any indirect participants, defined in the last paragraph of said II, permitting, in accordance with common rules and standardised procedures within the meaning of Directive 98/26/ EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, the regular execution of payments, through clearing or otherwise, and, for systems used for settlement and delivery of financial instruments, the delivery of securities between said participants.

The system must either have been instituted by a public authority or be governed by a framework agreement that respects the general principles of a market framework agreement or a model agreement. The Minister for the Economy sends the European Securities and Markets Authority a list of the systems having the benefit of Articles L. 330-1 and L. 330-2 governed by French law and their respective managers."

<sup>85</sup> We concur with Commission services that it is premature to envisage permissionless networks and decentralized platforms at current juncture.



- 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 or securities, or both)

However, the following aspect may hinder the designation as 'systems' by Member States:

- Legal changes at EU level on the qualification of the various types of 'crypto-assets', which may call for a revision of the SFD in order to explicitly encompass crypto-assets based on securities.

**Cash settlement:** 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 CSD 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. However it does not seem to be in conformity with the spirit of the regulation.

In the current state of the legislation, it would seem that the complete tokenization 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 CSD 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 CSD 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 tokenization 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.

To conclude, in the current state of the legislation, the development of security token platforms (only listed securities within the meaning of MiFID) providing settlement and delivery entirely on the blockchain **does not seem possible.**

Several legal obstacles can be identified.

In the current state of the legislation, security token platforms would have to go through the conventional banking system for the settlement of securities and through the various conventional post-trade intermediaries for their delivery (custodians, central securities depository authorisation).

If changes were considered, they should be undertaken both on the CFD Finality Directive (for derogations from bankruptcy law) and on the national level (recognition of the ownership of security tokens in the blockchain). Only such amendments could permit tokenization of the cash leg of settlement and delivery of security tokens and adapt the regulatory requirements to this new technology.

**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.**

**The AMF is of the view 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.**

The AMF's opinion is that 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.

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 in CSDR as an "account on which securities may be credited or debited". We nevertheless recall 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 maintained by 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 up to 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.** A clarification could be made by ESMA to state that records on a DLT can be equated to a book-entry, or a legal clarification could be done 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 French Monetary and Financial Code and the Commercial Code.

The use of DLT for securities non-admitted to the operations of a central depository is authorised since 2017.

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".**

	1	2	3	4	5	No opinion
Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system				4		
Rules on measures to prevent settlement fails			3			
Organisational requirements for CSDs				4		
Rules on outsourcing of services or activities to a third party		2				
Rules on communication procedures with market participants and other market infrastructures			3			
Rules on the protection of securities of participants and those of their clients				4		
Rules regarding the integrity of the issue and appropriate reconciliation measures					5	
Rules on cash settlement					5	
Rules on requirements for participation			3			
Rules on requirements for CSD links			2			
Rules on access between CSDs and access between a CSD and another market infrastructure		2				
Other (including other provisions of CSDR, national rules applying the EU acquis, supervisory practices, interpretation, applications...)		2				

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

The AMF does not identify any issue for most of the above-mentioned current rules, apart on how to adapt the account holding to the world of DLT.

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 traditional CSDs. On the other hand, some rules, such as for example the rules on CSD interoperability 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 some issues remain 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 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** 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 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 equate 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 tokenization 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 CSD 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<sup>86</sup>? 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.<sup>87</sup> **As things stand at present, it would therefore be necessary for security token platforms to go through another intermediary – the custodian – in addition to the CSD – 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 prevent to benefit fully from the productivity gains made possible by the blockchain.

**6. Settlement Finality Directive (SFD)**

The Settlement Finality Directive<sup>88</sup> 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".**

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

**Please explain your reasoning.**

The AMF is of the view that the main definitions of the SFD should be adapted in a DLT environment.

<sup>86</sup> Such as the requirements regarding the recording on an account with a custody account keeper outside a DLT environment

<sup>87</sup> Article L. 211-3 of the Monetary and Financial Code

<sup>88</sup> Settlement Finality Directive (98/26/EC)



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 CSDs 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.<sup>89</sup> 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.<sup>90</sup> 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).

---

<sup>89</sup> Article L. 330-1 of the Monetary and Financial Code: "I. – An interbank settlement system or system used for settlement and delivery of financial instruments consists of a national or international procedure which organises relations between at least three parties, not counting the system manager, defined in 5° of II of this article, nor any indirect participants, defined in the last paragraph of said II, permitting, in accordance with common rules and standardised procedures within the meaning of Directive 98/26/ EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, the regular execution of payments, through clearing or otherwise, and, for systems used for settlement and delivery of financial instruments, the delivery of securities between said participants.

The system must either have been instituted by a public authority or be governed by a framework agreement that respects the general principles of a market framework agreement or a model agreement. The Minister for the Economy sends the European Securities and Markets Authority a list of the systems having the benefit of Articles L. 330-1 and L. 330-2 governed by French law and their respective managers."

<sup>90</sup> Article L. 330-1 II 5° of the Monetary and Financial Code taken from the Settlement Finality Directive.



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.

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. Given the fact that creating a whole new legal framework for DLTs could be premature, **the AMF proposes to create a testing zone (Digital Lab) that could first enable private stakeholders to develop DLT solutions before setting up a new legislation (see Q107 for our proposal).**

**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<sup>91</sup>? Please explain your reasoning.**

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 chosen 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. 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;

---

<sup>91</sup> 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.

- 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.**

The AMF is of the view that, even if SFD does not constitute a legal barrier to security tokens, the current wording of the SFD is not adapted to DLTs. 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<sup>92</sup> 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<sup>93</sup>.

**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**

---

<sup>92</sup> Financial Collateral Directive (2002/47/EC)

<sup>93</sup> 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)

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

	1	2	3	4	5	No opinion
if crypto-assets qualify as assets that can be subject to financial collateral arrangements as defined in the FCD			3			
if crypto-assets qualify as book-entry securities collateral			3			
if records on a DLT qualify as relevant account			3			
Other						

**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?

**98) FCD sets out rules on conflict of laws. Would you see any particular issue with applying these rules in a DLT network<sup>94</sup>?**

The conflict of laws rules set out in the FCD – the law of the relevant account- shall be adapted to a DLT environment : 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.

---

<sup>94</sup> 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

Still, the AMF has 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)<sup>95</sup> 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.

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

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

---

<sup>95</sup> European Markets Infrastructure Regulation (648/2012/EU)

**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. The AMF 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".**

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

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

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?**

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).**

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.

**9. The Alternative Investment Fund Directive**

The Alternative Investment Fund Managers Directive<sup>96</sup> (AIFMD) lays down the rules for the authorisation, ongoing operation and transparency of the managers of alternative investment funds (AIFMs) which manage and/or market alternative investment funds (AIFs) in the EU.

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

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

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

<sup>96</sup> Alternative Investment Fund Managers Directive (2011/61/EU)



arrangements, including with respect to identifying, managing and monitoring the conflicts of interest;						
Employing liquidity management systems to monitor the liquidity risk of the AIF, conducting stress tests, under normal and exceptional liquidity conditions, and ensuring that the liquidity profile and the redemption policy are consistent;				X		
AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets;				X		
Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments.				X		
Other						

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

**1/ AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens:**

The provisions of the AIFMD concerning the appointment and duties of the depositary (Art. 21) do not seem to raise any issues if the AIF is invested in security tokens.

However, the custody of the Fund's assets raises a question in relation to Articles 21.8 and 21.12 of the Directive:

- the depositary must ensure the custody of the financial instruments included in the assets of the FIA. In this respect, it must ensure the custody of these financial instruments registered in a financial instruments account opened in its books and of the financial instruments physically delivered to it;
- for "other assets", the depositary verifies the ownership of the Fund and keeps an up-to-date register of the assets. This second category includes financial instruments that are only registered directly in the name of the Fund to the issuer or its agent (i.e. registered financial instruments) since they cannot be held in custody (art. 88.2 of the delegated regulation 231/2013 of 19 December 2012).

However, the depositary has different obligations depending on whether it holds financial instruments or "other assets" (art. 89 and 90 of the delegated regulation 231/2013 of 19 December 2012). In particular, the AIFMD provides that, in the event of a loss of the financial instruments held in custody, the depositary must return financial instruments of an equivalent type to the fund, except in certain specific cases where the depositary may waive this obligation of return (Articles 21.12 and 21.13). On the other hand, in the event of loss of "other assets", the Directive does not impose any obligation on the depositary to return them, since the depositary is not holding them.

To date, these AIFMD provisions do not raise any operational difficulties since French law provides that security tokens are subject to record keeping ("other assets" rules) and not to custody by the depositary. However, this raises questions for the protection of investors, since there is no obligation on the depositary to return them, and the issue of the depositary's liability regarding security tokens might arise. On the other hand, other States might require the depositary to hold security tokens, which could lead to difficulties for cross border activities.

Therefore, it appears that a clarification of the legal framework applicable to the custody of security tokens by the depositary of FIA would probably be necessary in order to provide sufficient legal security for this activity.

## **2/ 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:**

The AIFMD provides that the manager of a AIF shall use "at all times, adequate and appropriate human and technical resources that are necessary for the proper management of AIFs" (art. 18.1). In addition, the AIFM Delegated Regulation 231/2013 of 19 December 2012 provides that the AIF manager must implement and maintain operational an updated business continuity plan including, in particular, a data back-up system (art. 57.3). These provisions imply that when an AIF manager wishes to use security tokens, he must first update his business plan by justifying that he has the appropriate human and technical resources to control and supervise the use of security tokens and by updating his continuity plan.

In particular, regarding the system of conflict of interest management required to be set up by the AIF manager, there is no provision in the AIFM Directive that seems incompatible with the use of security tokens.

## **3/ 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;**

The AIFMD provides that the manager must use an appropriate liquidity management system and adopt procedures to track the liquidity risk of the AIF and ensure that the liquidity profile of the AIF's investments is consistent with its underlying obligations (Art. 16.1). This measure is specified by Articles 46 to 49 of the AIFM Delegated Regulation AIFM 231/2013 of 19 December 2012.

As mentioned above, when an AIF manager wishes to use security tokens, he will first have to update his program of activity, justifying that he has the appropriate human and technical resources, in particular his liquidity management system, to enable it to comply with its obligations in relation with the management of the AIF's liquidity.

## **4/ AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets:**

The AIFMD provides that the manager ensures that, for each AIF managed by it, appropriate and consistent procedures are established to conduct an appropriate and independent valuation of the assets of the AIF (art. 19.1). This measure is specified by Articles 67 to 74 of the delegated regulation AIFM 231/2013 of 19 December 2012.

Given the diversity of the assets in which an AIF under French law may invest (French law already allows assets as varied as financial instruments, receivables, savings bonds, promissory notes, mortgage notes, etc.) and which managers must be able to value, there is no difficulty in assessing the portfolio of an AIF composed of security tokens under the conditions set out in the AIFMD.

Article 67.2 of the AIFM Delegated Regulation provides, inter alia, that valuation policies and procedures shall require that the staff members who actually carry out the valuation of the assets are competent and address the specific investment strategies of the AIF and the assets in which the AIF could invest. Article 70 provides that the review of valuation methods must be carried out "before the AIF engages in a new investment strategy or invests in a new type of asset not covered by the existing valuation policy". These measures imply that, when an AIF manager wishes to use security tokens, he must first update its program of activity, justifying that he has the appropriate human and technical resources, in particular his policies and procedures for the valuation of AIF assets.

## **5/ Transparency and reporting provisions of the AIFMD legal framework requiring to report certain**

## information on the principal markets and instruments:

The AIFMD provides that the manager must regularly report to its Member State Authority the main markets and instruments on which it trades on behalf of the AIFs it manages (art. 24.1). This measure is specified in Article 110 of AIFM Delegated Regulation 231/2013 of 19 December 2012.

These disclosure requirements do not seem to raise any difficulty of application regarding security tokens and their platforms.

### **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).**

No, as long as the marketing of the AIF is limited to its national territory. **In the absence of European harmonization relating to the recognition of the ownership of financial securities on the block and to their custody regime, the cross-border marketing of units or shares of mutual funds in the form of security tokens does not seem possible under the existing provisions.**

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

The UCITS Directive<sup>97</sup> 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".**

---

<sup>97</sup> Undertaking for Collective Investment in Transferable Securities Directive (2009/65/EC)

	1	2	3	4	5	No opinion
Provisions of the UCITS Directive pertaining to the eligibility of assets, including cases where such provisions are applied in conjunction with the notion “financial instrument” and/or “transferable security”		X				
Rules set out in the UCITS Directive pertaining to the valuation of assets and the rules for calculating the sale or issue price and the repurchase or redemption price of the units of a UCITS, including where such rules are laid down in the applicable national law, in the fund rules or in the instruments of incorporation of the investment company;				X		
UCITS Directive rules on the arrangements for the identification, management and monitoring of the conflicts of interest, including between the management company and its clients, between two of its clients, between one of its clients and a UCITS, or between two -UCITS;					X	
UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;			X			
Disclosure and reporting requirements set out in the UCITS Directive.					X	
Other						

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

**1/ Provisions of the UCITS Directive pertaining to the eligibility of assets, including cases where such provisions are applied in conjunction with the notion of “financial instrument” and/or “transferable security”**

Article 50 of the UCITS Directive lists the assets in which a UCITS may invest, including transferable securities.

The qualification of security tokens as transferable securities depends on the rights attached to them (financial rights and political rights). Thus, a case-by-case analysis must be carried out on each token in order to determine its legal qualification. The AMF considers that, as long as the token confers financial rights of which the corresponding financial flows are paid to the holder of the security by the issuer of the security or an entity related to it, it can be qualified as a transferable security within the meaning of MiFID. However, most of the security tokens studied to date by the AMF have hybrid characteristics.

Therefore, **it might be useful for the UCITS Directive to specify, if that is the objective, that security tokens are eligible for UCITS assets, setting out the conditions, if applicable, and the proportion of such security tokens.**

**2/ 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;**

Article 85 of the UCITS Directive provides that “The rules for 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 shall be

laid down in the applicable national law, in the fund rules or in the instruments of incorporation of the investment company.”

A priori, no provision of French law is incompatible with the valuation and the rules relating to the issue and redemption of units or shares of a UCITS whose assets are composed of security tokens. It should be noted that Article 5 of the implementing directive 2010/43/EU of 1 July 2010 requires the UCITS management company to employ "staff with the necessary qualifications, knowledge and expertise to carry out the responsibilities entrusted to it". These measures imply that, when a UCITS management company wishes to use security tokens, it must first update its programme of operations, justifying that it has the appropriate human and technical resources, in particular its rules for valuing the assets of the UCITS.

### **3/ 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**

The UCITS Directive provides that the UCITS management company must be structured and organised in a way that minimises the risk that conflicts of interest between the company and its clients, between two of its clients, between one of its clients and a UCITS or between two UCITS may harm the interests of the UCITS or its clients (Art. 12.1). Articles 17 to 21 of Implementing Directive 2010/43/EU of 1 July 2010 sets out the conflict of interest mechanism that must be implemented by UCITS management companies. These provisions do not seem incompatible with the use of security tokens by a UCITS.

### **4/ UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens**

Please refer to our answer to Question 105 above on FIA's depositary (Point 1).

The relevant provisions concerning the UCITS depositary are Articles 22.5 and 24 of the UCITS Directive and Article 12 of the UCITS Delegated Regulation 2016/438 of 17 December 2015.

### **5/ Disclosure and reporting requirements set out in the UCITS Directive**

We understand that the question refers to the obligations of UCITS management companies regarding investor information under Articles 68 to 82 of the UCITS Directive. These disclosure requirements do not seem to be incompatible with the use of security tokens by a UCITS. It should be noted that in this case, the information given to investors will have to be adapted in all disclosure documents: the prospectus will have to specify that the UCITS is invested in this type of assets (Art. 70.1) and that the volatility of the portfolio is therefore high (Art. 70.3), advertising communications on these investments will have to be correct, clear and not misleading (Art. 77), the DICI will have to indicate the risk profile of the UCITS as a result of these investments (Art. 78.3), etc.

## **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).**

1. CREATION OF A EUROPEAN DIGITAL LABORATORY

Regulatory changes would be necessary at the European and national levels to enable the development of token security platforms without the use of the traditional banking system for the settlement of securities nor the various current post-trade intermediaries for their delivery (custody account keepers, central depository). These developments became necessary since traditional financial regulation is designed to require the use of intermediaries who provide a guarantee to investors as financial market professionals, whereas blockchain makes it possible to dispense with these intermediaries. Only these changes, combined with guarantees adapted to this new technology, would ultimately make it possible to take full advantage of the productivity gains resulting from the possible disintermediation offered by the blockchain.

However, the market for intermediation services on digital assets is growing very fast as there are many participants organizing the relationship between the different blockchains, trading platforms and investors. Therefore, it is possible that the market will organise itself in a similar way as for all types of financial instruments, with the rise of actors offering a full range of services to investors.

If it were considered to suggest regulatory changes at the European level, two avenues could be put forward : (i) the amendment of European texts in which obstacles to the development of security tokens were identified, even if the security token environment is still not very mature and the regulators do not have the necessary hindsight to propose the relevant amendments; (ii) the creation of an ad hoc regulation for security tokens in order to take into account the specificities of the blockchain and its decentralised nature, given the lack of maturity of the market, such a regulation is difficult to create.

An alternative approach could consist in suggesting the implementation of a mechanism at the European level allowing the competent national authorities to waive certain requirements imposed by European regulations and identified as incompatible with the blockchain environment, as long as the entity benefiting from this exemption complies with the key principles of the regulations and is subject to increased supervision by the competent national authority of the reference Member State.

Such a mechanism would require the implementation of a governance process at the European level to ensure that the competent national authorities can discuss and harmonize their practices.

Such a mechanism would remove the regulatory obstacles to the emergence of token security market infrastructure projects that would be able to be developed in a secure environment, without modifying all European regulations, which could take place at a later stage, once the ecosystem has matured and by relying on the expertise that the competent national authorities would have gained from the guidance of companies.

The foreseeable impact of the exemptions granted on the current organisation of the financial markets should be assessed. Indeed, it is highly conceivable that market participants transfer their activities to a blockchain in order to get rid of the existing regulatory rules. In this respect, it will be necessary to define



precisely what a blockchain is in order to avoid a "blockchain-washing" phenomenon, with some participants pretending to operate on blockchains that in reality are not.

**This European exemption mechanism, which could be qualified as a digital laboratory, would be implemented by a level 1 European text (regulation or directive) that would provide possible derogations, criteria, compensatory measures for regulatory exemptions and their duration.** This mechanism could have the following characteristics.

#### 1.1 Texts subject to the exemption

**Certain financial instruments traded on a platform would be exempted from CSDR regulation and even from certain provisions of MiFID II identified as unsuitable for the blockchain environment.** This would make it possible, for small-scale projects, to test the possibility of creating token security trading platforms without the need to go through a central depository whose authorisation seems (i) cumbersome, (ii) unsuitable for blockchain technology and smart contracts which allow, to a certain extent, the automatization of operations classically carried out by a central depository while maintaining a high level of security, (iii) impossible to implement at this stage given the absence of available tokenised central bank money.

#### 1.2 Scope of the financial instruments covered by the exemption

All the financial instruments defined by MIF directive would be eligible as long as they are listed on the blockchain. This would take the following form:

- **Financial instruments listed in Section C of Annex 1 of MiFID II that are issued, registered, recorded, stored or transferred in digital form by using distributed registry technology would be eligible for the experimentation;**
- **Distributed registry technology should be conceived as a way to ensure the registration, integrity and permanence of registrations and to enable, directly or indirectly, the identification of the owners of securities and the nature and number of securities held<sup>98</sup>.**

The implementation of the European experimentation should obviously not lead to the emergence of systemic risks, therefore limits in terms of emission and trading volumes must be introduced. **It is suggested that the liquidity thresholds defined in MIFIR be used as a basis. Thus, only financial instruments not considered liquid within the meaning of MiFID would be eligible for the exemption. Article 4.17 b) of MIFIR sets three criteria to define the liquidity of a financial instrument: (i) the free float for shares and the issue volume for bonds, (ii) the average daily number of transactions, (iii) the average daily trading volume.** These criteria are quantified for each financial instrument in delegated regulations. For example, a share is considered illiquid if its free float is less than €200 million, if the average daily number of transactions is less than 250 and if the average daily trading volume is less than €1 million.

This approach has several benefits:

- It is based on a European text in force;
- It is exhaustive as it concerns all financial instruments;
- The thresholds concern both the issue volumes that limit the primary market and the trading volumes that limit secondary market activity;
- These thresholds are both non-systemic and, simultaneously, important enough to ensure that the experimentation is not just a simple "proof of concept" area (POC) but allows for the development of real European offers.

#### 1.3 Authorisation of the competent authorities

---

<sup>98</sup> The ESMA opinion on ICOs and crypto-assets of 9 January 2019, defined the blockchain as follows: "Distributed Ledger Technology (DLT) is a means of saving information through a distributed ledger, i.e. a repeated digital copy of data available at multiple locations".



**Project developers wishing to benefit from all or part of the exemptions should request authorisation from a national competent authority.**

This authorisation would be conditioned to the communication to the regulator of (i) a business plan, (ii) a request for exemption on EU regulations explicitly specified in the authorisation request and (iii) a description of the technical and contractual arrangements implemented to ensure that the parties involved in the project comply with the key principles of the provisions from which they derogate, in particular with regard to customer protection. For example, regarding settlement, stipulating an "atomic swap" system through a smart contract, which only allows securities to be exchanged for settlement when it is certain that both counterparties possess both, is likely to reduce counterparty risk and justify the granting of an exemption to CSDR regulation.

**Could be involved in a project and apply for an authorisation under the conditions set out above:**

- **Entities that are already regulated and authorised** to provide investment and payment services, and, where applicable, those authorised under specific national authorisation such as the PSANs in France;
- **Non-regulated entities that present guarantees in terms of good repute and organisation equivalent to those required for regulated entities.**

As the goal is to test specific projects, the authorisation request should be sought at the project level, with the relevant stakeholders. Thus, a stakeholder who has joined the experimentation wishing to carry out a second project should apply for an additional authorisation.

In addition, **a continuous dialogue between the project leader and the competent authority should be set up throughout the duration of the experimentation.** Supervision by the competent authority could take the form of notifications of operations, ad hoc or regular reporting, as necessary depending on the activity carried out by the project leader. If necessary, actors running private blockchains could join the supervisor via the transmission of an auditor node.

#### 1.4 Coordination at the European level

In order to avoid regulatory arbitrage and to promote convergence between Member States, a coordination process should be set up at European level, which could be implemented by ESMA. **A supervision of the experiments should be carried out by ESMA, in a format to be defined,** in order to gather sufficient data to feed a review report of the system for the European Commission after 3 years and a comprehensive reporting of the experiments.

#### 1.5 AML-CTF rules and market abuse

It should be specified that **the experimentation will, under no circumstances, exempt actors from complying with the AML-CTF regulation.** In the same way, the Market Abuse Regulation is applicable under its ordinary legal conditions.

#### 1.6 The experimental framework in time

**A 3-year review clause could be introduced in the regulation in order to determine, at the end of this period, whether the experimentation should be continued or whether sufficient information has been gathered to allow the amendment of the existing texts in order to adapt them to the blockchain technology.**

It should be noted that **the United States has adopted an identical approach to the proposed experimentation. A "no-action letter" was published by the SEC on 28 October 2019 concerning Paxos,** authorising it not to be registered as a clearing agency for its securities settlement activities on a private blockchain under certain conditions, including the volume of transactions settled, the formalisation of procedures to govern the experiment, regular reporting to the SEC and a maximum duration of the experiment limited to two years.

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

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 and in particular does not lead to preventing experiments involving public blockchains as it cannot be excluded at this stage that the development of blockchain technologies will follow in the footsteps of the Internet, i.e. the emergence of a decentralized technology on a global scale (Internet) and the development of many applications for more private use (e.g. intranets).

Our experience at the AMF at this stage indicates that there are both serious projects involving open and decentralised blockchains and others based on a closed blockchain approach.

Decentralized platforms again raise more questions from a regulatory point of view and are hardly compatible with our current frameworks. Nevertheless, given the growing success of decentralised finance ("DeFi") applications, we believe that it is more appropriate to support the development of this segment in a secure manner rather than trying to combat it.

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).**

It seems difficult to answer this question when in fact this regulatory separation exists. We are faced with 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?**

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

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

**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).**

### **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)<sup>99</sup> sets out the rules for the business practices and supervision of e-money institutions.

In its advice on crypto-assets<sup>100</sup>, 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<sup>101</sup> (PSD2). PSD2 puts in place comprehensive rules for payment services, and payment transactions. In particular, the Directive sets out rules concerning a) strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud; b) the transparency of conditions and information requirements for payment services; c) the rights and obligations of users and providers of payment services.

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

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

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

---

<sup>99</sup> Electronic Money Directive (2009/110/EC)

<sup>100</sup> [EBA report with advice for the European Commission on "crypto-assets"](#), January 2019

<sup>101</sup> Payment Services Directive 2 (2015/2366/EU)

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

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 *"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"*. 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 devices, *"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**
- **Don't know/no opinion**

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

No, but some actors may need to ask both for PSP license and for crypto-asset provider license which 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 EMIs. 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 EMIs 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 EMIs only to avoid KYC costs although their activity has a similar risk profile as PIs. 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 were 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").**

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

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

We consider that stablecoins consist in an “asset-backed” issuance insofar 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 stablecoin users possess a claim on the stablecoins themselves and on their underlying assets.

For example, we believe that Libra could be considered as an asset-backed stablecoin 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 stablecoins (should be more important). If global stablecoins 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 stablecoins to fit into the e-money definition. Consequently, stablecoins’ issuers and service providers would have to abide by EMD2 prudential requirements, which we consider to be suitable for safeguarding stablecoin 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)?**

Completely appropriate	<input type="checkbox"/>
Rather appropriate	<input type="checkbox"/>
Neutral	<input checked="" type="checkbox"/>
Rather inappropriate	<input type="checkbox"/>
Completely inappropriate	<input type="checkbox"/>
Don't know / No opinion	<input type="checkbox"/>

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

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

\*

\* \*

## Abbreviations

AIF – Alternative Investment Fund

AIFM – Alternative Investment Fund Manager

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

AML/CFT – Anti-Money Laundering/ Combatting the Financing of Terrorism

AMLD5 – 5<sup>th</sup> Anti-Money Laundering Directive (Directive 2018/843/EU)

BCBS – Basel Committee on Banking Supervision

CCP – Central Clearing Counterparty

CDS – Credit Default Swap

CSD – Central Securities Depositories

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

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

DLT – Distributed Ledger Technology

DMD – Distance Marketing of Consumer Financial Services Directive (2002/65/EC)

EBA – European Banking Authority

ECB – European Central Bank

EIOPA - European Insurance and Occupational Pensions Authority

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

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

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

ESCB – European System of Central Banks

ESMA – European Securities Market Authority

ETF– Exchange-Traded Fund

EU- European Union

FATF – Financial Action Task Force

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

FSB – Financial Stability Board

ICO – Initial Coin Offering

ICT – Information Communication Technologies

IPO – Initial Public Offering

ISIN – International Securities Identification Number

LEI – Legal Entity Identifier

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

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

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

MTF – Multilateral Trading Facility

NCA – National Competent Authority

OTC – Over the Counter

OTF – Organised Trading Facility

P2P – Peer-to-peer

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

PR – Prospectus Regulation (2017/1129/EU)

RM – Regulated Market

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

SME – Small Medium Enterprise

STO – Security Token Offering

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

TR – Trade Repository

UCITS – Undertaking for Collective Investment in Transferable Securities

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

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

### Definitions

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

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

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

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

are publicly known and essential for identification, and private keys, which are kept secret and are used for authentication and encryption.

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

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

**E-money token:** For the purpose of the consultation, e-money tokens are a type of 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.