ADAN

L'ASSOCIATION POUR LE DÉVELOPPEMENT DES ACTIFS NUMÉRIQUES

ADAN's contribution

European Commission's consultation on an EU framework for markets in crypto-assets

v.1

Paris, le 19 mars 2020

Introduction

ADAN is a 1901 non-profit organisation whose mission is to bring together and animate the digital assets industry in France and in Europe. With 20 corporate members, including Ark Ecosystem, Blockchain Partner, Coinhouse, Coinhouse Custody Services, ConsenSys France, iExec, Kaiko, Ledger, LGO Markets, Nomadic Labs and Woorton, ADAN is the most important French organization in the digital assets field.

The ADAN is thankful to the European Commission for allowing the expression of industry players in this open consultation. The Association's objectives are to help create the more favourable environment in the EU for the development of a crypto-asset industry competitive with other regions of the world. The Association is available for any additional commentary or work related to the subjects covered by this consultation.

The content of this answer is formally supported by the Financial Instrument Global Identifier (FIGI) Working Group on the Identification of crypto-assets.

Contacts:

- Simon Polrot, President: simon.polrot@adan.eu
- Faustine Fleuret, Head of Strategy and Institutional relations: faustine.fleuret@adan.eu

Website: www.adan.eu

Twitter: @adan_asso

Media Kit: https://adan.link/presskit

Table of contents

I. Question for the general public

1. Have you ever held crypto-assets?

ADAN does not hold any crypto-assets.

2. If you held crypto-assets, what was your experience?

N/A

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

As a non-profit association advocating for the development of blockchain and crypto-assets industry, ADAN may in the future hold any crypto-assets.

The reasons for holding crypto-assets as a non-profit association may be: accepting membership fees paid in cryptocurrencies or stablecoins, paying for services on blockchain-based applications, paying service providers that only accept crypto-assets as a means of payment, or investing excess treasury.

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

We want to be able to accept those crypto-assets as soon as possible. It is currently very difficult for companies and associations to hold crypto-assets and maintain good relationships with their banks. As soon as this problem is alleviated for all the companies operating in France (which is one of the missions of the ADAN), we will allow members to pay for their membership fees in crypto-assets.

II. Classification of crypto-assets

General comments

Comment on the "crypto-assets" definition of the European Commission

We agree with the European Commission's approach. Our opinion is that "crypto-assets" are defined:

- through a technological angle (registered on a DLT), and
- by their general characteristics (a digital asset being purely digital, permanent, non-duplicable and directly apprehensible).

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

Comment on the "crypto-assets" classification

We agree with the detrimental effect that the lack of convergence on the classification of crypto-assets has to progress into debates and discussions. There is a crucial need of definition and harmonisation so that under any concepts everyone talks about the same thing.

1) Crypto-assets that qualify as existing legal instruments should not be subject to another new qualification. However, legal adjustments are necessary to take into account the guarantees brought by the technological features of crypto-assets (in terms of efficiency, security, reliability, privacy,

liquidity, etc.) and adapt rules, either because they cannot prevail in crypto-asset markets or to make them simpler thanks to blockchain benefits.

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

To conduct such analysis, ADAN supports the French financial regulator's approach to create a "**digital laboratory at European level** allowing the national competent authorities to remove, in return for appropriate guaranties, certain requirements imposed by European regulations and identified as incompatible with the blockchain environment, provided that the entity benefiting from this exemption respects the key principles of the regulations and that it is subject to increased surveillance by the national competent authority of the reference Member State"[1].

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

2) **For crypto-assets that do not qualify under current legislations**, categorization purely based on their economic functions prove some limits. That is why a class of "hybrid tokens" had to be defined to cover evolving tokens and those that do not easily fit into one category. When it comes to regulating them, many characteristics should help distinguish them and their regulatory regime.

a) Functionally speaking, crypto-assets can be distinguished as follows:

- "**cryptocurrencies**" i.e crypto-assets governed by the blockchain protocol itself (e.g bitcoin, ether).

Cryptocurrencies are crucial to the well-functioning of the public blockchain they are native from. They are used as economic incentives for validators to make the network run, and are considered as good ways to transfer value for all the participants to the network. As they are ruled by the protocol that defines all their technical characteristics, they are not controlled by a single central operator. They are traded on a peer-to-peer basis.

A transaction in cryptocurrencies is valid if the blockchain protocol is respected. The correct execution of the protocol is guaranteed by the validating nodes.

Their economic function is not determined by a specific issuer. Instead, different groups of participants of the networks use them for different economic functions: payment, investment, collateral, store of value...

Therefore, we consider that those multipurpose assets have to be analyzed as forming a new class of assets.

- "**tokens**" or "**programmable crypto-assets**" i.e crypto-assets deployed on the blockchain by its owner(s) who is/are the identified issuer(s) of these tokens and who determines its characteristics.

[1] https://www.amf-france.org/en/news-publications/news/legal-analysis-application-financial-regulations-security-tokens-and-precisions-bulletin-board

Contrary to cryptocurrencies, programmable assets do not participate in running the blockchain. They are not ruled by the protocol, as they are issued by one or several identified persons that encrypt the features of their tokens in smart contracts. Therefore they are a very eclectic asset class (see b) below).

A transaction in tokens is valid if a person sends a transaction that meets the conditions encrypted by the issuer.

b) Tokens are a very heterogeneous asset class. In fact they could all qualify as “hybrid”. The main characteristics of such tokens enable to establish their wide variety:

- the type of network on which they are issued (public or private),
- the level of control* and centralisation,
- their fungible or non-fungible nature,
- whether they are representative of a legal right,
- whether they are necessarily associated with another asset existing outside of the blockchain (goods, real estate, etc.),
- their level of complexity (how many functions does the token entail? e.g.: a token used for payment as an ERC20 is very simple, whereas a token that governs a DAO as the MakerDAO token can be complex).

	Cryptocurrencies	Tokens or programmable crypto-assets		
		Utility tokens (access to a service run on blockchain)	Digital representation of one real asset (e.g a luxury bag)	Stablecoins
Fungible	✅	✅ or ❌	❌	✅
Native	✅	✅	❌	✅[2] or ❌[3]
Control	-	- à +++	++	+++
Complexity	+	++	++	+++

[2] Some algorithmic stablecoins (e.g. DAI stablecoin).
[3] Issued by a private party, commercial or central banks.

*Token standards usually define the level of control. For example, smart contracts deployed with specific standards (such as the well-used ERC20) are controlled by the bearer, not by the issuer. Others are controlled by the issuer, and in this case the latter has control over all transfers of tokens that he issued. Thus, even if an investor has lost his key or if a transaction identified as fraudulent by means of a stolen key, the issuer could possibly return the tokens to its rightful owner by canceling the said transaction ("force transfer" function).

Liabilities borne by issuers of programmable crypto-assets can be easy or difficult to determine depending on their level of control over the tokens. For example, they are more difficult to assess in the case of tokens that are not controlled by the issuer than for the ERC 20 standard controlled by the issuer.

c) Based on the previous findings, **building large categories of crypto-assets seems non-practical (since to be really representative, there should be many) and inefficient from a regulatory point of view.** That is why for those who do not fall within any existing legal definition, the best approach is likely:

- distinguish “cryptocurrencies” from all other forms of tokens (as they have a unique set of characteristics), and
- establish a broad “(programmable) crypto-asset” or “tokens” class and to define a scalable regulatory framework in which very granular requirements would be (or not) applicable depending on:
    - the technological features of the crypto-asset: cryptocurrency or programmable asset,
    - its inherent characteristics: native or not, fungible or not, etc. (see b) above),
    - the activity/services operated on such crypto-assets,
    - their economic function(s),
    - a risk analysis of the combination of all these elements, that is comparing the risk profile of the actor with the guarantee that they provide regarding: financial stability, user protection, fair competition.

“Crypto-assets” that do not qualify under existing legislation should then be analyzed on a case-by-case basis and a bottom up logic. **This should be the function of a <u>new regulatory or self-regulatory body dedicated to crypto-asset markets</u>.**

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

In consequence, we are in favor of a two-level legal analysis:

- A legal analysis and regime at the level of the assets, as described above, that would help categorize each and every asset based on their sets of characteristics;
- A legal analysis and regulatory regime at the level of the actors dealing with the crypto-assets in general, in order to ensure a significant level of professionalism, ethics and integrity in market practices, security, AML/CFT procedures, etc. - which corresponds to the definition and

regulation of so-called « VASPs » as defined by the FATF or the « PSAN » in the French legislation.

Therefore there are requirements that would apply regarding the type of crypto-assets whereas others would apply regarding the service/activity provided on such assets.

Questions

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.

The scope of this consultation should be limited to crypto-assets. Most arguments are based on the characteristics allowed by the underlying DLT, then could not be valid under other assumptions.

Our opinion is that “crypto-assets” are defined:

- through a technological angle (registered on a DLT), and
- by their general characteristics (a digital asset being purely digital, permanent, non-duplicable and directly apprehensible).

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

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

Yes.

The classification of crypto-assets should lay the foundations for their regulation. This means that the rationale behind the definition of one category of crypto-assets should be the existence or the necessary creation of its specific regulatory regime.

To this end, crypto-assets that qualify with existing legal instruments should not lead to the creation of other categories.

For crypto-assets that do not fit into any existing legal concepts, two qualifications should be created:

- “cryptocurrencies” for crypto-assets that are governed by the blockchain protocol itself,
- “tokens” or “(programmable) crypto-assets” for those which are issued by an identified person (or several) and whose main features are determined by the issuer(s).

A flexible framework should be built upon very granular requirements. The application of each provision would depend on:

- the technological features of the crypto-asset: cryptocurrency or programmable asset,
- its inherent characteristics (see General comments point b) above),
- the activity/services operated on such crypto-assets,
- a risk analysis of the combination of all these elements, that is comparing the risk profile of the actor with the guarantee that they provide regarding: financial stability, user protection, fair competition.

This approach seems pragmatic and close to the reality behind the great heterogeneity of crypto-assets. In our opinion, a classification based solely on economic considerations could not be the best option as it has already proved insufficient (hybrid tokens, evolving tokens, some tokens do not easily fit into one category). See answer to question 8.

"Crypto-assets" that do not qualify under existing legislation should then be analysed on a case-by-case basis and a bottom up logic. **This should be the function of a <u>new regulatory or self-regulatory body dedicated to crypto-asset markets</u>.**

Moreover, regarding the potential of crypto-assets for great and fast evolutions, coupled with the lack of history of this young ecosystem, **new legal mechanisms should enable flexibility and possible fast changes, at least during the first years of this regime**.

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).

Among those which do not qualify under any existing legal concept, the classification of crypto-assets should consider their technological foundation. That is why "cryptocurrencies" and "(programmable) crypto-assets"/"tokens" should be distinguished. Then the activity/service provided on such crypto-assets, their intrinsic features and their risk profile should help define among a set of rules which regulatory requirements should apply.

As a point of reference, in France, crypto-assets are classified under the following two categories:

- Crypto-assets that qualify as "digital assets" under the new PACTE regime. "Digital assets" encompass both ICO "tokens" and "virtual currencies" defined in AMLD5. Based on the functional analysis described above, this would include cryptocurrencies and a wide range of programmable tokens.

> Article L. 552-2 of the French Monetary and Financial Code defines a "token" as "any intangible asset representing, in digital form, one or more rights that can be issued, registered, stored or transferred by means of a shared electronic recording device making it possible to identify, directly or indirectly, the owner of said asset"
>
> Art. L. 54-10-1 of the French Monetary and Financial Code defines "digital assets" as:
> "1° The tokens mentioned in article L. 552-2, excluding those fulfilling the characteristics of the financial instruments mentioned in article L. 211-1 and the "bons de caisse" mentioned in article L. 223 -1;
> 2° A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically"

- Crypto-assets that do not qualify as "digital assets" under the new PACTE regime.
    - This explicitly covers tokens that qualify as financial instruments (as established in the "digital assets" definition) and "bons de caisse"[4].

[4] Defined in article L. 223-1 of the French Monetary and Financial Code

- This implicitly refers to any other crypto-assets that do not fit into the “digital assets” definition, such as for example non-fungible tokens and stablecoins.

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

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

In consequence, we are in favor of a two-level legal analysis:

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

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’?

No.

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

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

Moreover, the traditional categorisation shows some flaws:

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

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?

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

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

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

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

Please justify your reasoning.

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

We would like to emphasise the importance of two opportunities:

- improved transparency and traceability of transactions is a very strong attribute of public blockchain-based use cases that can bring benefits to various transactions executed on blockchain at the stage of execution but also and especially after the execution stage. It has

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

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

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

	1	2	3	4	5	N/A
Fraudulent activities		■				
Market integrity (e.g. price, volume manipulation, ...)			■			
Investor/consumer protection				■		
Anti-money laundering and CFT issues			■			
Data protection issues		■				
Competition issues		■				
Cyber security and operational risks				■		
Taxation issues		■				
Energy consumption entailed in crypto-asset activities		■				
Financial stability		■				
Monetary sovereignty/monetary policy transmission		■				

Please justify your reasoning.

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

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

Second, risks depend on the activities/services provided on these crypto-assets. For instance, ML-FT risks are much weaker regarding crypto-crypto exchanges than crypto-fiat exchanges (see below). That

is why a meaningful risk analysis requires a more granular case-by-case approach to better reflect the heterogeneity of crypto-assets.

“Fraudulent activities” is a very broad concept which can potentially refer to many various topics, that is why it seems difficult to appraise a general level of risk.

“Anti-money laundering and CFT issues” exist but should not be overstated. AML-CFT issues have been analysed by the French Treasury in its national report on ML-FT risks published in september 2019. If they observe that crypto-assets can (practically) be diverted from their right use in order to circumvent AML-CFT regulations, the French authority qualifies their risk score as “moderate” (on a scale from “weak” to “high”). Some of their arguments are:

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

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

12. In your view, what are the benefits of “stablecoins” and “global stablecoins”?

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

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

Stablecoins are programmable “money”. Programmability and automation could optimise the delivery versus payment (DvP) of transactions. According to a decentralized model, crypto-assets and payment assets are usually entered into an “escrow smart contract” until the two players confirm that they agreed upon their trading conditions. If such conditions are met, the smart contract automatically triggers the exchange of assets. Conversely, if the smart contract does not receive confirmation from the parties or contradictory information from the seller and the buyer, the smart contract does not execute the transaction and send back assets to each party (crypto-assets for the seller, the settlement asset for the buyer). That is why decentralized DvP requires both assets and means of payment to be “tokenized“ to ensure the atomic execution of transactions. Otherwise, if the cash leg is not managed on chain, DvP involves that the off chain “cash leg” and the on chain “crypto-asset” leg of transactions are executed

simultaneously, which can be very complex to implement. Stablecoins could then allow to fully process transactions on blockchain.

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

“Retail stablecoins”, issued for individuals, could allow under- or even unbanked to overcome the difficulties encountered in order to transfer funds between individuals. Stablecoins fall within the growing trend of recent years to the digitization of cashless payments, led notably by Google, Apple, Facebook and Amazon. These new means of payment, which can be easily used with a mobile phone, support greater financial inclusion for populations where the banking system and payment infrastructures are the least efficient (or even do not exist). Today 1.7 billion adults are unbanked but 1.1 billion have a mobile phone (two thirds of them) and, in developing economies, 44% of adults use digital payments[5]. In addition, the programmability of those assets would allow for the use of blockchain-based applications with high levels of security, reliability, auditability and transparency.

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

Fraudulent activities	1	2	3	4	5	N/A
Market integrity (e.g. price, volume manipulation, ...)			■			
Investor/consumer protection		■				
Anti-money laundering and CFT issues			■			
Data protection issues				■		
Competition issues	■					
Cyber security and operational risks			■			
Taxation issues	■					
Energy consumption entailed in crypto-asset activities	■					
Financial stability			■			
Monetary sovereignty/monetary policy transmission				■		

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

[5] Figures from the World Bank’s Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution : https://openknowledge.worldbank.org/bitstream/handle/10986/29510/211259ovFR.pdf?sequence=5&isAllowed=y

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

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

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

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, a bespoke regime for crypto-assets (that are not currently covered by EU financial services legislation) is crucial to enable a sustainable crypto-asset ecosystem in the EU. Legal uncertainty is detrimental to the long-term vision of business then prevents from the broad adoption of crypto-assets. This is also the opportunity for the EU to set a clear and favourable regulatory land where Asia and North America have not taken the lead yet.

But this regime should meet some essential conditions to be able to inspire confidence for users and business partners with the crypto industry while allowing actors to foster their innovative potential. To this end, proportionality, efforts to move away from traditional regulations that can inspire regulatory works, and granularity in determining roles and responsibilities of new actors are critical.

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

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

An alternative to such legislative texts could be the creation of a “28th regime”. Recital 14[6] of the Rome 1 Regulation allows for designing an “optional instrument” (or “28th regime”) that would be a second regime “providing parties with an option between two regimes of domestic contract law”[7]. According to

[6] “Should the Community adopt, in an appropriate legal instrument, rules of substantive contract law, including standard terms and conditions, such instrument may provide that the parties may choose to apply those rules.”
[7] Opinion of the European Economic and Social Committee on “The 28th regime — an alternative

article 3 of the Rome 1 Regulation, parties can choose the law by which their contract shall be governed. In this scenario, national regimes when there are (such as the French PACTE Law) could co-exist with an EU crypto-asset regime.

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.

The French regulatory regime on crypto-assets

Promulgated on 22 May 2019, the "PACTE[8] law" provides an innovative regulatory framework for some actors of the crypto-asset industry and their supervision by French financial regulators (AMF and ACPR). These actors are:

a) token issuers
b) digital asset service providers ("PSAN").

a) The French Financial Markets Authority (AMF) can issue an "ICO" visa for an offering when the token issuer complies with some underlying requirements, mainly relating to the content of the white paper and promotional marketing materials, the monitoring and safeguarding of the assets (both legal money and crypto-assets) collected all along the ICO and anti-money laundering and counter-financing of terrorism.

This visa is optional, meaning that token issuers are not prohibited to launch their ICO to the French public if they do not ask for the visa or do not obtain it. However, the visa provides some advantages. The most relevant one for actors today is the unrestricted access to banking services: they cannot be refused access by credit institutions to deposit and payment account services. For such a refusal, or if they did not answer to the actor's request by 2 months, credit institutions must provide the AMF and the ACPR with the reasons for this refusal. The ACPR can offer actors the possibility to ask the French Central Bank for appointing one credit institution to provide required services.

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

Even if this is an optional visa, the AMF has some prevention-based method of abuses:

- Withdraw of an ICO visa - temporarily or definitively - if the issuer no longer complies with the ICO visa conditions,
- "Black list": list of ICOs that have had their approval withdrawn or have published misleading information about the issue of the approval,

allowing less lawmaking at Community level" (own-initiative opinion): https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AC%3A2011%3A021%3A0026%3A0032%3AEN%3APDF

[8] Action Plan for Business Growth and Transformation

- “Name and shame” any issuer who communicates unfair, unclear or misleading information to the public regarding the ICO visa issuance or its implications.

Once the AMF grants its visa, the white paper is published online by both the issuer - 2 days maximum once he got the visa - and the AMF who updates the “white list” of ICOs that were granted its visa. The white paper is valid 6 months maximum and during the whole duration of the ICO.

After issuing tokens, issuers must provide their writers with the following information:

- Assets collected from the ICO 2 days maximum after the end of the ICO: amount of assets collected, number of tokens issued, token allocation between categories of owners, amount of assets collected and already used (when appropriate),
- Annual information to client about the use of asset collected,
- (If any) Secondary market options.

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

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

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

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

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

Article L. 54-10-2 of the French Monetary and Financial Code defines “digital asset services” as:
1° Custody of digital assets
2° Buying or selling digital assets against legal money (“crypto-fiat exchange”)

3° Exchange of digital assets with other digital assets (“crypto-crypto exchange”)
4° Operation of a digital asset trading venue
5° Other services on digital assets such as:
- RTO on behalf of clients
- Portfolio management
- Investment advice
- Underwriting on a firm commitment basis
- Placing on a firm commitment basis
- Placing without a firm commitment basis

The regulation of PSANs is based on two regimes:

b.i) The mandatory registration of certain types of providers (services 1° and 2°),
b.ii) The optional license of any service provider, if they request it.

So if all PSAN can - but are not forced to - ask for the AMF license, those who conduct digital asset custody and crypto-fiat exchange activities must register with the Authority (“PSANs 1 and 2”).

b.i) Without being registered, “PSANs 1 and 2” are prohibited from providing crypto-custody or crypto-fiat exchange.

To be registered, “PSANs 1 and 2” must comply with the following provisions:

- Honorability and competence of managers
- Honorability, competence and sound and careful management by individuals that have a supervisory power
- AML-CFT

Once registered, “PSANs 1 and 2” are added to the public list held by the AMF.

Like token issuers stamped by the AMF, “PSANs 1 and 2” that are registered with the AMF benefit from the unrestricted access to banking services.

b.ii) Without getting the license, PSANs are NOT prohibited from providing their services, except if “PSANs 1 and 2” are not registered with the AMF. However, the license constitutes a guarantee of credibility, a competitive advantage and a business argument.

To get the license, PSANs must comply with a common condition package for all service providers, but also to some specific rules depending on services that they offer. The common rules are the following:

- General information, notably: name, address, contact point, list of services that will be provided with and without a license, identity of shareholders and (natural or legal) persons who can exercise a significant influence over the management of that company, incorporation document
- Financial information, notably: the current financial position of the applicant, forecast data, financial statements for existing companies;
- Professional liability insurance or own funds;
- Safety and internal control system;
- Resilient and secure IT system;
- Conflicts of interest management system;

- Fair, clear and not misleading information to clients (including about risks related to digital assets);
- Publication of their pricing policy;
- Efficient claim management policy.

Once they have the license, PSANs are added to the public list held by the AMF.

Like token issuers stamped by the AMF, PSANs that got the AMF license benefit from the unrestricted access to banking services.

ADAN comments on the French regime

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

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

However, they might be some possible improvements:

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

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)

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

- **Flexibility and scalability**. As stated above, the traditional categorization of crypto-assets (payment, investment, utility and hybrid tokens) should be dropped. A better approach seems to distinguish crypto-assets that legally qualify under current regulations from others. Within "others", "cryptocurrencies" and "tokens/(programmable) crypto-assets" should be subject to

adjustable requirements depending on the activity/service provided, the intrinsic features of assets and their risk profile.

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

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

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

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?

In general, harmonisation of laws within the European Union is a favorable evolution for any business. If at this stage, ADAN did not deeply investigate this topic lacking the required expertise, our preliminary conclusion is that convergence in national civil laws could facilitate inherently cross-border activities on crypto-assets within the European Union, and even galvanize intra-EU synergies.

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

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?

The French regime for crypto-assets set rules for both token issuers and digital asset service providers (PSAN). See answer to question 15.

Article L.552-3 of the French Monetary and Financial Code defines the issuance of crypto-assets as "an offer of tokens to the public [that] consists of offering the public, in whatever form, to subscribe to these tokens. The offer of tokens open to subscription to a limited number of persons [150 people] acting on their own account does not constitute an offer of tokens to the public."

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

Article L. 54-10-2 of the French Monetary and Financial Code defines "digital asset services" as:

1° Custody of digital assets;

2° Buying or selling digital assets against legal money (“crypto-fiat exchange”);

3° Exchange of digital assets with other digital assets (“crypto-crypto exchange”);

4° Operation of a digital asset trading venue;

5° Other services on digital assets such as:

- RTO on behalf of clients;
- Portfolio management;
- Investment advice;
- Underwriting on a firm commitment basis;
- Placing on a firm commitment basis;
- Placing without a firm commitment basis.

1. Issuance of crypto-assets

1.1 Issuance of crypto-assets in general

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?

Not necessarily.

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

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

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

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-assets

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…)

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

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

The “white paper” should contain minimum information about:

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

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)?

	1	2	3	4	5	No opinion
The Consumer Rights Directive						

The E-Commerce Directive						
The EU Distance Marketing of Consumer Financial Services Directive						
Other (please specify)						

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

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

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?

	1	2	3	4	5	No opinion
The managers of the issuer or sponsor should be subject to fitness and probity standards						
The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions						
Where necessary, the issuer or sponsor should put in place a mechanism to safeguard the funds collected such as an escrow account or trust account						
Other						

Please explain your reasoning.

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

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

- First, token issuers cannot be refused access by credit institutions to deposit and payment account services[9]. For such a refusal, or if they did not answer to the actor's request by 2 months, credit institutions must provide the French authorities (the AMF and the ACPR) with the reasons for this refusal. The ACPR can then offer actors the possibility to ask the French Central Bank for appointing one credit institution to provide required services.
- Second, their tokens become eligible assets for some investment vehicles (up to a 20% threshold).

1.2 Issuance of "stablecoins" backed by real assets

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...)?

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

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?

	"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...)				
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				

[9] French Monetary and financial code, art. L. 312-23 and D. 312-23

The assets or funds of the reserve should be segregated from the issuer's balance sheet				
The assets of the reserve should not be encumbered (i.e. not pledged as collateral)				
The issuer of the reserve should be subject to prudential requirements rules (including capital requirements)				
The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating				
Obligation for the assets or funds to be held in custody with credit institutions in the EU				
Periodic independent auditing of the assets or funds held in the reserve				
The issuer should disclose information to the users on (i) how it intends to provide stability to the "stablecoins", (ii) on the claim (or the absence of claim) that users may have on the reserve, (iii) on the underlying assets or funds placed in the reserve				
The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically				

Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer					
Other					

Please illustrate your response.

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

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

Trading platforms

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?

	1	2	3	4	5	No opinion
Absence of accountable entity in the EU						
Lack of adequate governance arrangements, including operational resilience and ICT security						
Absence or inadequate segregation of assets held on the behalf of clients (e.g. for 'centralised platforms')						
Conflicts of interest arising from other activities						

Absence/inadequate recordkeeping of transactions		■				
Absence/inadequate complaints or redress procedures are in place			■			
Bankruptcy of the trading platform			■			
Lacks of resources to effectively conduct its activities	■					
Losses of users' crypto-assets through theft or hacking (cyber risks)				■		
Lack of procedures to ensure fair and orderly trading			■			
Access to the trading platform is not provided in an undiscriminating way	■					
Delays in the processing of transactions	■					
For centralised platforms: Transaction settlement happens in the book of the platform and not necessarily recorded on DLT. In those cases, confirmation that the transfer of ownership is complete lies with the platform only (counterparty risk for investors vis-à-vis the platform)			■			
Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse		■				
Other						

Please explain your reasoning.

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

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

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

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

	1	2	3	4	5	Comment
Trading platforms should have a physical presence in the EU			■			This presence would be necessary for the control of AML/FT procedures.
Trading platforms should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)		■				
Trading platforms should segregate the assets of users from those held on own account				■		They do.
Trading platforms should be subject to rules on conflicts of interest			■			
Trading platforms should be required to keep appropriate records of users' transactions			■			For centralized entities.
Trading platforms should have an adequate complaints handling and redress procedures				■		
Trading platforms should be subject to prudential requirements (including capital requirements)		■				Should be adapted to the nascent nature of the industry.
Trading platforms should have adequate rules to ensure fair and orderly trading			■			
Trading platforms should provide access to its services in an undiscriminating way			■			

Trading platforms should have adequate rules, surveillance and enforcement mechanisms to deter potential market abuse						
Trading platforms should be subject to reporting requirements (beyond AML/CFT requirements)						
Trading platforms should be responsible for screening crypto-assets against the risk of fraud						
Other						

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

No.

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

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

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

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

	1	2	3	4	5	Comment
Absence of accountable entity in the EU						
Lack of adequate governance arrangements, including operational resilience and ICT security						
Conflicts of interest arising from other activities						
Absence/inadequate record keeping of transactions						

Absence/inadequate complaints or redress procedures are in place						
Bankruptcy of the exchange						
Inadequate own funds to repay the consumers						
Losses of users' crypto-assets through theft or hacking						
Users suffer loss when the exchange they interact with does not exchange crypto-assets against fiat currency (conversion risk)						
Absence of transparent information on the crypto-assets proposed for exchange						
Other						

Please explain your reasoning.

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

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

	1	2	3	4	5	Comment
Absence of accountable entity in the EU						
Exchanges should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)						

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

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

Provision of custodial wallet services for crypto-assets

31. In your opinion, what are the main risks in relation to the custodial wallet service provision? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1	2	3	4	5	Comment

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

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

No.

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

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

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

- Security: The custodian can lose access to the funds of the customer due to a hack, theft, etc...
- Technical: The custodian can lose access to the funds due to a technical mistake, shutdown, hardware or software malfunction, physical loss of any document where the private keys can be stored, etc…
- Governance: if the governance is badly defined or controlled, the control of the funds can be lost by the relevant party.

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

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

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

	1	2	3	4	5	Comment
Custodial wallet providers should have a physical presence in the EU	■					
Custodial wallet providers should be subject to governance arrangements (e.g. in terms of operational resilience and ICT security)			■			
Custodial wallet providers should segregate the asset of users from those held on own account				■		

Custodial wallet providers should be subject to rules on conflicts of interest	■					
Custodial wallet providers should be required to keep appropriate records of users' holdings and transactions	■					
Custodial wallet providers should have an adequate complaints handling and redress procedures			■			
Custodial wallet providers should be subject to capital requirements		■				
Custodial wallet providers should be subject to advertising rules to avoid misleading marketing/promotions	■					
Custodial wallet providers should be subject to certain minimum conditions for their contractual relationship with the consumers/investors				■		
Other						

32.1 Is there any other requirement that could be imposed on custodial wallet providers in order to mitigate those risks?

Please specify which one(s) and explain your reasoning:

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

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

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

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

That is why it seems important for the development of an European industry of custodians that regulations applying to them be the most consistent possible whatever the type of crypto-assets is. First, one client is likely to hold different legal types of crypto-assets on one single private key. Therefore

this could be very detrimental to European actors wishing to design an attractive offer if complying with too divergent rules according to different crypto-assets appears very burdensome. Second, custody of crypto-assets whatever they are legally qualified requires the same technical expertise and arrangements. It would make few sense that requirements in terms of security, safeguarding, reporting, etc. be different.

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?

As we advocate that crypto-assets that comply with the MiFID II "financial instrument" definition must fall within the same regulatory package, this implies that custodian that provides "safekeeping and administration of financial instruments for the account of clients, including custodianship and related services such as cash/collateral management and excluding maintaining securities accounts at the top tier level"[10] must be authorised by the national competent authority.

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

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

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

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

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

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

[10] MiFID 2, appendix 1 section B.

account or the account of another client with clear, full and accurate information on the obligations and responsibilities of the custodian

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

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?

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

5. Other service providers

35. In your view, what are the services related to crypto-assets that should be subject to requirements? (When referring to execution of orders on behalf of clients, portfolio management, investment advice, underwriting on a firm commitment basis, placing on a firm commitment basis, placing without firm commitment basis, we consider services that are similar to those regulated by Annex I A of MiFID II.) Please rate from 1 (completely irrelevant) to 5 (highly relevant)

	1	2	3	4	5	Comment
Reception and transmission of orders in relation to crypto-assets						
Execution of orders on crypto-assets on behalf of clients						
Crypto-assets portfolio management						
Advice on the acquisition of crypto-assets						
Underwriting of crypto-assets on a firm commitment basis						
Placing crypto-assets on a firm commitment basis						

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

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

No.

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

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

The two services "reception and transmission of orders in relation to crypto-assets" and "execution of orders on crypto-assets on behalf of clients" do not illustrate the current functioning of crypto-assets

markets. There is currently no use of such services and defining a regulatory framework for these providers should not be a priority.

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

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

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

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?

No, in general. This is especially the case since we consider that none of the payments made using crypto-assets are using services "making payment transactions".
Payments by crypto-assets are usually done using two distinct means:

- A professional directly accepts crypto-assets as a means of payment. In this case, the client sends the crypto-assets to the seller's account on the blockchain. The seller keeps the assets or later sells them against other assets or fiat currency.
- A professional is using a service to accept crypto-assets, that will take the payment on his behalf, convert the crypto-asset to fiat currency, and give them the proceeds of the sale minus a commission.

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

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

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

III.C Horizontal questions

1. Market integrity

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

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

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

N/A

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

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

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

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

- the multinational nature of those crypto-assets that allows for trading in any jurisdiction, and

- the existence of decentralized or semi-decentralized services that operate without limitations and without prior identification of clients.

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

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

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

39. Do you see the need for supervisors to be able to formally identify the parties to transactions in crypto-assets? If yes, please explain how you would see this best achieved in practice.

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

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

- The crypto-assets can be sold and bought anywhere in the world. Most assets are listed either outside of the EU or both inside or outside of the EU. There's no easy path for a cross-border regulation that would allow EU supervisors to ask foreign exchanges for that information, especially where those exchanges do not ask for any identification of clients (this practice is still common for exchanges between crypto-assets).
- More and more exchanges between crypto-assets are done through decentralized exchanges. Those exchanges are operated directly on the blockchain and provide two distinct sets of features: they are accessible from anywhere and to anyone, and all the trades are executed publicly on the blockchain and are auditable by a third party.

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?

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

2. AML/CFT

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)?

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

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

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

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.

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

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

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?

No. See answer above.

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

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

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

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

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?

	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						
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						

Please explain your reasoning.

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

However, it has to be noted that those requirements should be adapted as follows:

- the AML/CFT training should be, as much as possible, adapted to the crypto-asset industry specifically;

- the cost of compliance to those two requirements should be low (in order to avoid the creation of significant barriers to entry to this nascent market). In this regard, the creation of reference documents and training delivered by the regulator or a professional organization for a low price would help.

3. Consumer/investor protection

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

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

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

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

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

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

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?

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

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?

No, information provided should be identical.

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)?

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

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

	1	2	3	4	5	No opinion
Those crypto-assets should be banned	■					
Those crypto-assets should be still accessible to EU consumers/investors					■	
Those crypto-assets should be still accessible to EU consumers/investors but accompanied by a warning that they do not necessarily comply with EU rules	■					

Please explain your reasoning.

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

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

4. Supervision and oversight of crypto-assets service providers

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).

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

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

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

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

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

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

IV.A General questions on "security tokens"

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

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

Please explain your reasoning.

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

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

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

Completely agree	
Rather agree	
Neutral	
Rather disagree	
Completely disagree	
Don’t know / No opinion	

Please explain your reasoning.

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

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

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

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

Please explain your reasoning.

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

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

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

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

IV.B Assessment of legislation applying to “security tokens”

1. MiFID II

1.1 Financial instruments

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

Completely agree	
Rather agree	
Neutral	
Rather disagree	
Completely disagree	
Don’t know / No opinion	

Please explain your reasoning.

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

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

60. If you consider that this is an impediment, what would be the best remedies according to you?

	1	2	3	4	5	No opinion
Harmonise the definition of certain types of financial instruments in the EU						
Provide a definition of a security token at EU level						

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

Please explain your reasoning.

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

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

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)?

	1	2	3	4	5	Comment
Hybrid tokens should qualify as financial instruments/security tokens						Hybrid tokens should qualify as “tokens/(programmable crypto-assets”
Hybrid tokens should qualify as unregulated crypto-assets (i.e. like those considered in section III. of the public consultation document)						But should not be left unregulated.

The assessment should be done on a case-by-case basis (with guidance at EU level)						"Crypto-assets" that do not qualify under existing legislation should be analysed on a case-by-case basis and a bottom up logic. This should be the function of a new regulatory or self-regulatory body dedicated to crypto-asset markets.
Other						

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

1.2 Investment firms

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

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

Please explain your reasoning.

In any aspect of regulation, legal certainty is favourable for the economic development of an industry. If at this time ADAN did not deeply analyse the whole regulatory package applying to investment firms and its appropriateness in the context of security tokens, it is likely that new actors on the market on

financial instruments will have questions and expect clarifications from regulators. That is why this could be quite efficient to anticipate such questions.

1.3 Investment services and activities

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

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

Please explain your reasoning.

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

One key problem is the structuration of secondary markets for security tokens. Not all exchanges can fit into one of the proposed services listed for operating a venue. Such is the case, firstly, of decentralized platforms. For all types of crypto-platforms, as participants are usually individuals, being qualified as regulated markets or multilateral trading facilities (MTF) or organised trading facilities (OTF) would create regulatory frictions considering the requirements that participants must be authorized entities.

Moreover, reception and transmission of orders and execution of orders do not illustrate the current functioning of crypto-assets markets. There is currently no use of such services and defining a regulatory framework for these providers should not be a priority.

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

1.9 Access to trading venues

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

Today, individuals are granted direct access to crypto-exchanges and are not intermediated by another actor. This allows faster transactions and cost-reduction (especially regarding brokerage fees).

When trading security tokens, the opportunity to involve the same intermediaries as for traditional financial markets should be questioned regarding the additional guarantees in terms of security, liquidity, transparency, etc. brought by DLT.

This risk-analysis could be one aspect of the work that the “digital laboratory at European level” promoted by the AMF should conduct.

4. Prospectus Regulation (PR)

4.2 The drawing up of the prospectus

83. Do you agree that Delegated Regulation (EU) 2019/980 should include specific schedules about security tokens? If yes, please indicate the most effective approach: a “building block approach” (i.e if 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.

Yes. The content of the prospectus should be adapted to the specificities of security tokens.

On the one hand, under the current legislation, some crucial information is missing to enable potential subscribers to make informed decisions. On the other hand, parts of the content of the prospectus is also relevant for security tokens. That is why a “building block approach” seems the most effective approach.

Among information that we consider that potential subscribers of security tokens should be aware in order to better realize the characteristics and risks of an STO, might appear in the prospectus those that relate to: the underlying technology and its risks, the characteristics and the rights attached to the tokens, as well as details in the event of subscription of crypto-assets (instead of or in addition to a traditional subscription in current currency legal).

First, if security tokens are financial instruments within the meaning of MiFID II, the fundamental difference lies in the blockchain technology on which they are based. This is why it seems logical to specify its specific characteristics and risks. The issuer should thus describe the underlying technologies used, and the technical specifications such as architecture, protocol, and standards they could have used. Complete information would also go through the detailed description of the general and specific technological risks of the underlying technology(ies) selected by the issuer, and through the presentation of the risks linked to asset transfers, cyber-criminality and possible blockchain vulnerabilities. More "technologically savvy" subscribers may wish to consult the computer program used for the functional issue / description, or even its certification by a competent third party when the issuer requests it.

Compared to a traditional initial public offering, STOs have specific characteristics and rights attached to security tokens which are specific to crypto-assets. On the one hand, the technology on which the tokens will be registered and, if applicable, the technology on which the issuer intends to migrate the tokens after issuance should be presented. On the other hand, the modalities of transmission of the tokens and, where applicable, the intention of the issuer to request their admission on an exchange platform.

Regarding this last point, the information currently requested under the prospectus should be adapted to the reality of security tokens. Indeed, article 7.7.b of the Prospectus Regulation requires the issuer to indicate whether the financial tokens will be traded on an organized market, namely a regulated

market or a multilateral trading facility (MTF). Thus, the text as it stands does not take into account the other possible negotiation methods for digital assets, such as the use of a decentralized platform or the peer-to-peer exchange of security tokens.

Finally, if applicable, the prospectus should provide details in the event of subscription to digital assets (cryptocurrencies or stablecoins), which issuers of financial tokens can request in place of or in addition to a traditional subscription in legal tender currency. Then, the terms of payment-delivery could be clarified, as well as the mechanisms of storage of the digital assets collected: the means of collection and monitoring of the assets, the description of the systems of follow-up and safeguard of the assets received, or even the policy currency risk management and the conditions under which the issuer intends to convert crypto-assets into foreign currency. Also, the process of possible return of the assets to their subscribers should be presented, clarifying the repayment terms and the device for managing the exchange risk at the time of this repayment.

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

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

If you agree, please indicate if ESMA's guidelines on risk factors should be amended accordingly. Please explain your reasoning.

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

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

5. Central Securities Depositories Regulation (CSDR)

92. In your Member State, does your national law set out requirements to be taken into consideration, e.g. regarding the transfer of ownership? Please explain your reasoning.

In France, the two "Blockchain decrees" constituted a first step towards tokenization of financial assets by allowing the use of distributed ledgers for the issuance, registration, and transfer of some securities instead of traditional securities accounts (giving the samel legal effects, such as the transfer of ownership):

- The "Blockchain decree" No. 2016-520: for "mini-bons" that is a class of short-term debt instrument dedicated to the financing of SMEs;

- The “Blockchain decree” No. 2017-1674: for securities that are not admitted to the operation of a Central Securities Depository (non-listed Equity, transferable debt securities, shares of collective investment undertakings)

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

8. European Markets Infrastructure Regulation (EMIR)

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

Completely agree	
Rather agree	
Neutral	
Rather disagree	
Completely disagree	
Don’t know / No opinion	

Please explain your reasoning.

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

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

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

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

11. Other final comments and questions as regards security tokens

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? If yes, please explain the regulatory approach that you favour. Please explain your reasoning.

Yes. The EU legislation should provide for more regulatory flexibility for stakeholders to develop trading and post-trading solutions using for example permissionless blockchain and decentralised platforms.

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

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

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

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

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

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

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? If yes, please identify the issues that should be addressed at EU level and the approach to address them. Please explain your reasoning.

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

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? Please provide specific examples (national provisions, implementation of EU acquis, supervisory practice, interpretation, application, ...) and explain your reasoning for your answer to question 112.

The two “Blockchain decrees” described above (see answer to question 92) do not cover security tokens that are admitted to trade to the operation of a Central Securities Depository, that is those that are tradeable on secondary markets.