FESE response to the European Commission consultation on crypto-assets

Brussels 19th March 2020

Classification of crypto-assets

Q5 - Do you agree that the scope of this initiative should be limited to crypto-assets (and not be extended to digital assets in general)?

☒Yes
☐No
☐Don't know / no opinion/not relevant

Please explain your reasoning (if needed).

The approach to a definition should be focused on the features of the assets themselves, instead of the technology that enables them. FESE would support a broad definition that: could cover assets that do not yet have a defined regime, does not introduce additional burdens to current compliance requirements and maintains technology neutrality.

A commonly, binding legislative approach, based on existing EU financial market regulations would provide much needed legal certainty to reduce regulatory arbitrage, inconsistencies and market fragmentation and ensure scalability of services within the EU. This would place the EU as a global international standard setter that embraces innovation.

Technology neutrality and "same business, same risks, same rules" should apply to uphold the principles of transparency, fairness, stability, investor protection and market integrity.

It is important to have clarification on EU level that where "digital-assets" qualify as financial instruments these will be subject to already existing financial market rules. This would increase the speed to market for innovations, as market participants and authorities would act within a well-established legal framework and rules would be appropriate for institutional and retail investors. Such clarification should be provided in alignment with global standard setting bodies like ISO.

There is a need for one single EU classification that covers the representation of "digital-assets" as defined in the scope of this consultation as "any text or media that is formatted into a binary source and includes the right to use it." As other categories of digital assets are thinkable, the classification should refer to those services and activities related to these assets.

FESE agrees that a particular focus should be given to "crypto-assets" that represent the assets with the most immediate potential for DLT application in financial markets and therefore are in need of regulatory clarification and solutions. FESE believes that the creation of an EU classification of "digital-assets" should a) define a "crypto-asset" as a "digital asset" based on cryptography and b) introduce a clear distinction between "crypto-assets" that represent the digitalised embodiment of a 'traditional asset' or act

as financial instruments and "digital-assets" that do not. The classification would include clear and distinct categorisation of security-, payment-, utility- and hybrid "crypto-assets".

Based on this, it would be determined if a given "digital-asset" would fall under the definition of a "crypto-asset" and be subject to the existing EU regulative framework.

Q6 - In your view, would it be useful to create a classification of crypto-assets at EU level?

☒Yes
☐No
☐Don't know / no opinion/ not relevant

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

FESE favours a regulatory categorisation at EU level. This would allow regulators and financial market participants to have a common definition of "digital asset" and allow distinguishing between different types to bring significant benefits to market participants and consumers.

FESE supports the introduction and application of a harmonised regime. On a general line, FESE would not favour the use of "soft law" (e.g. guiding principles), as this might be interpreted differently by Member States. FESE, therefore, welcomes that the Commission is considering potential regulatory requirements to address "crypto-assets" currently not covered by EU legislation. Moreover, we believe that 'investment/security tokens' should be considered as financial instruments under MiFID II (Article 4, paragraph 15). Alternatively, such clarification could potentially be given through Level 2 amendments. However, any legislative measures should avoid undermining other potentially applicable regulations (such as EMD for certain payment tokens). In line with the Better Regulation principles, we consider it important that any changes to the definitions of financial instruments be subject to an impact assessment to avoid any unintended consequences.

Q7 - 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).

The categorisation of "crypto-assets" should not be based on different technical features provided by cryptography and DLT technology but on the value of the assets represented. This means that if a category of "crypto-assets" represents a financial instrument defined in MiFID II under Annex I, Section C of the MiFID II (1)-(11), then these assets should be treated as such instruments (e.g. if the represented value is a share, then all rules for shares shall apply, if the represented value is a commodity, then all rules for commodities shall apply). If a hybrid "crypto-asset" contains elements of a financial instrument (at any point of its life-cycle), it should fall under the financial rules for the respective financial instrument.

"Crypto-assets" which are currently not covered by definitions of financial instruments should be integrated in the MiFID II definition of financial instruments. We would propose to define a category "other digital-assets" as a new point (12) under Annex I, Section C of MiFID II. Moreover, 'investment/security tokens' should be considered as financial instruments under MiFID II (Article 4, paragraph 15).

It is necessary to have a taxonomy for "crypto-assets" that is effectively based on the rights and obligations stemming from the asset. "Crypto-assets" should thus be classified according to the nature of the asset, irrespective of the technology used for creating,

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

evidencing and transmitting the rights associated to the asset. Specifically, for "crypto-assets", we suggest to include a differentiation based on whether the asset is native (created on DLT), or tokenised (backed by real or tangible assets).

Most importantly, from a financial market integrity and investor protection perspective, is that a classification of "digital assets" introduces a clear differentiation between "digital assets" that act as financial instruments (i.e. "crypto-assets") and "digital assets" that do not act as a financial instrument. This clarification should help identify which regulations that will apply to these different types of products and to the Financial Market Infrastructures where they are available.

The classification of "crypto-assets" should enable:

(i) Uniform interpretation of qualifications and criteria on what constitutes different forms of "crypto-assets", taking into account the technology related features (for example, in respect of transferability, how temporary lock ups, selling/ contractual restrictions or utility rights can be exercised in the use of a "crypto-asset").

(ii) Identification of the specific class of security (share, bond or other) – by accounting for attributes such as 'legal claim vs counterparty'.

Q8 - Do you agree that any EU classification of crypto-assets should make a distinction between 'payment tokens', 'investment tokens', 'utility tokens' and 'hybrid tokens'?

☒Yes
☐No
☐Don't know / no opinion/not relevant

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

FESE agrees that any EU categorisation of "crypto-assets" should make a distinction between the different types of tokens using the blockchain technology. This would provide further clarify on the scope of future Commission initiatives which should aim to remain limited to "crypto-assets.".

FESE welcomes the EU's proposed distinction between 'payment tokens', 'investment tokens', 'utility tokens' and 'hybrid' tokens as they capture the various branches of "crypto-assets". Regulations should apply based on the type of tokens, which differ based on their functionality (e.g. investment tokens pose risks to investor protection, whilst utility tokens would pose risks to consumer protection, which are two different regulatory compliance frameworks).

FESE believes that this presents an opportunity to better clarify the distinction between "digital-assets" that act as financial instruments using cryptology (i.e. "crypto-assets") and "digital-assets" that do not act as financial instruments and use cryptology" (which could be defined as "crypto-tokens").

For example, an 'investment token' - which is defined as a token with "profit-rights attached to it" should be defined as a financial instrument under the existing regime to establish trust in the nascent "crypto-assets" market whilst preserving investor protection.

'Utility tokens' which do not fulfil the criteria of a financial instrument, should still be treated in such a way that investors are protected, and markets are fair, efficient and transparent (see e.g. IOSCO objectives of Securities Regulation) and be considered as a "crypto-token".

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Therefore, for the purpose of this consultation, please note that references to 'investment/security tokens' in our answers refer to "crypto-assets" that act as financial instruments as defined in the current regulatory framework for financial markets as provided by MiFID II Article 4, paragraph 15.

Q9 - Would you see any crypto-asset which is marketed and/or could be considered as 'deposit' within the meaning of Article 2(3) DGSD?

N/A

Crypto-assets that are not currently covered by EU legislation

Q10 - In your opinion, what is the importance of each of the potential benefits related to crypto-assets listed below?

Please rate each proposal from 1 to 5, 1 standing for "not important at all" and 5 for "very important".

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

Q10.1 - Is there any other potential benefits related to crypto-assets not mentioned above that you would foresee?

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

FESE considers that it is important to establish key principles upon which the EU can build a role in facilitating the development and implementation of FinTech. These principles include the need for:

•The application of the same rules for the same services and risks (including across different pieces of legislation) based on the principle of technology neutrality

•A risk-based approach built on proportionality and materiality which allows for flexibility, particularly in respect of innovation with small groups of customers (i.e. sandboxes), while ensuring a level playing field across the EU

•A balancing of the local (country) risks alongside the benefits of cross-border markets (i.e. scalability, interoperability and passporting of services).

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q10.2 - Please justify your reasoning for your answers to question 10.

Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs:

ICOs (Initial Coin Offerings) are not and should not be seen as "a cheaper more efficient capital raising tool" than traditional IPOs as the structuration of any offering implies the intervention of specialists (legal, finance, etc.) for the issuance's success. Hence, the ICO costs are broadly the same as for any other types of offering. Based on industry consultation, costs of ICOs amount on average to 1 EUR million. This amount mostly depends on the size and importance of marketing and the willingness of project owners to comply with regulators overseas or only in a dedicated region.

Utility tokens should not be considered investment tools, but rather an alternative to crowdfunding. In this sense, FESE agrees that utility tokens can be considered an alternative to current capital raising schemes, with particular interest for start-up companies that do not meet the standards for accessing traditional funding from investors through the current tools.

On the contrary, IPOs hold several benefits for companies and investors such as: enabling sustainable, long-term growth, lowering overall funding costs and enhances a company's profile and reputation as listing is a quality mark in terms of transparency and governance. Moreover, listing on public markets entails complying with extensive disclosure requirements, producing a prospectus and following rules in relation to investor protection.

FESE shares ESMA's concerns regarding investor protection (specifically whether investors are aware of the level of risk involved) and firms conducting business without applying EU legislation in the context of crypto assets and ICOs.

FESE is also concerned with regard to data protection issues and their relation to DLT environments, as the immutability of this technology and impossibility to delete data prevent these systems to deal with personal data safely, and therefore do not allow for complying with the requirements laid out in GDPR.

Even for permissioned DLT, confidentiality of data can only be guaranteed by keeping satellite records in traditional technologies that ensure personal information can be erasable, which does not contribute to the overall safety of the information and adds complexity and costs to the maintenance of the system.

We consider that if the same economical background exists then these tokens should be classified as investment tokens (and follow financial market rules). In an own initiative report, the ESMA Securities and Markets Stakeholders Group (SMSG) underlines the importance of legal certainty in ICOs and "crypto-assets". The report points to the need for clarification regarding the application of existing financial regulation to virtual (crypto) assets. Such clarification is necessary given the very divergent national regulatory approaches to "crypto-assets". FESE therefore welcome that the Commission is considering potential regulatory measures to address "crypto-assets" currently not covered by EU legislation.

Issuance of utility tokens as an alternative funding source for start-ups: Utility tokens can be used as an alternative way for start-ups to fund specific projects / products, notably by attracting a community of investor-user from the start of their funding growth process. However, since tokens, and the rights attached to them, are essentially difficult to understand for a wide audience, there are limits and obstacles for them to be used as the main vehicle to fund start-ups.

"Crypto-assets" as a new investment opportunity for investors: "crypto-assets" may provide new investment opportunity to investors, notably by providing investor access to early stage (small-ticket) projects compared to what would be required for a typical seed financing round for similar type of projects.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Improved transparency and traceability of transactions: It is important to address this point as "crypto-assets" do not provide improved transparency compared to standard instruments, due to the difficulty to find reliable information on the asset themselves (issuer disclosures can be fallacious) and in regards to trading volumes (likewise, public information can be manipulated, with "fake" transaction undertaken by "crypto-asset"-trading platforms for instance). However, in theory, "crypto-assets" should provide for greater traceability than standard financial instruments, as the recording of investor activity is essential to the technology (on the primary and secondary markets) and are recorded immutably on a ledger.

Enhanced innovation and competition: Indeed, "crypto-assets" are enhancing innovation and competition, due to their potential to streamline the instrument lifecycle management, the transaction chain and to provide alternative funding and investment vehicle for start-ups.

Q11 - In your opinion, what are the most important risks related to crypto-assets? Please rate each proposal from 1 to 5, 1 standing for "not important at all" and 5 for "very important".

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

Q11.1 - Is there any other important risks related to crypto-assets not mentioned above that you would foresee?

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

With an EU framework, the risks mentioned above could be mitigated. Besides "classic" risks of new asset-classes (fraud, money laundering, market manipulation) technology related "new" risks such as energy consumption, finality, integrity of the network, "right to be forgotten" and application of GDPR provisions arise.

Some DLT forms, such as public blockchains have no legally accountable entity to be held liable for failing to implement risk management procedures to address the risks mentioned above, which is a risk by itself. We would recommend policies and procedures to be followed by entities that wish to offer their products and services to "retail clients" or offer securities to the public.

There are specific risks arising from smart contracts e.g. in the case of unintended programming of the algorithm within such a smart contract. A trusted third party would help to prevent or mitigate such risks from occurring e.g. by providing certified smart contracts and ensuring their execution. So-called smart contracts should ideally follow a general standard and be certified. Such standards could be set at the EU level but should be aligned with international bodies and developed with market participants.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q11.2 - Please justify your reasoning for your answers to question 11:

Fraudulent activities: Fraudulent activities constitute an important issue. Due to the absence of regulation, "crypto-assets" have been used as vehicles for fraudulent activities, notably scams. It is important to note that there are specific types of fraud linked to "crypto-assets". "Crypto Frauds" are composed of various forms of cyber-attacks and electronic robberies which might result in the loss of users or investors' assets.

Market integrity (e.g. price, volume manipulation): There are important suspicions of market abuse on "crypto-assets"' secondary markets, including regarding the publication of "fake" orders and transactions by "crypto-asset"-trading platforms willing to attract more liquidity via the use of price manipulation. "Crypto-asset"-trading platforms are also acting as receptors / transmitters of client orders and are dealing on their own account on the same trading platform. This can have an impact on other instruments using the concerned "crypto-asset" as an underlying.

Investor/consumer protection: As mentioned in question 10, the key risks for investors / consumers relate the absence of reliable information regarding the "crypto-asset" per se and their strong exposures to the risks of fraud and market manipulation. It is an important concern, as "crypto-assets"-trading platforms are directly accessible by retails investors and several huge frauds have shown how retail users and investors are vulnerable.

Money Laundering /Financing terrorism is the first risk for operators and service providers with "crypto-assets". This has been pointed out by financial intelligence units as a growing risk. It is currently considered that a very large amount of "crypto-assets" are manipulated by groups involved in money laundering or terrorism financing. It is worth noting that the EU 5th AML directive has included "crypto-assets" services providers in its scope.

Data protection issues: There are data protection risks if the public key can be traced back to an actual person/entity. FESE is particularly concerned about the implications of DLT networks for investor protection and market abuse. The lack of transparency and potential illiquidity of "crypto-assets", make final investors particularly vulnerable to fraudulent manipulation of prices; current EU legislation targets these areas and offer a very high degree of investor protection as present market infrastructures are subject to their requirements.

Data protection is an area of great concern as compliance with GDPR is not guaranteed in all DLT networks, as well as cyber resilience, especially when considering the possibility of cyber-attacks.

Cyber security and operational risks: There are cyber security and operational risks related to blockchain in itself and to off-chain mechanisms (custody of "crypto-assets" notably).

Energy consumption entailed in crypto-asset activities: Even if new protocols are being designed to solve this issue, blockchain technology consumes more energy than centralised infrastructures (from proof of work to proof of stake for instance.

Considering the very important risks above, market integrity will be a major concern for platform operators. We would like to take this opportunity to again emphasise the need to have clear definitions of the different branches of "crypto-assets" and to identify the regulatory frameworks they should be subjected to.

As a minimum, comprehensive definitions of security / investment and hybrid tokens should be provided across the EU.

Moreover, the risks related to "crypto-assets" strongly depend on the functionality and governance behind the technology. Different level of risks may occur depending on, i.e.

- Type of "crypto-assets" (and underlying regulation)
- Open vs. permissioned networks and technology (i.e. identity)

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

- Underlying technology, i.e. smart contracts

That said, these risks are similar to those associated with current (financial) business processes.

Q12 - In our view, what are the benefits of "stablecoins" and "global stablecoins"? Please explain your reasoning.

FESE believes that the use of stablecoins should be clarified in the framework of EU post-trade regulations, notably in the scope of the CSDR. The issuance of stablecoins, at a national or European level, could solve existing CSDR-related issues by introducing a "delivery against payment" system using blockchain technology. Stablecoins can provide price stabilisation by linking the value of the coin to the value of a pool of assets whilst possessing the capability to serve as a means of payment. (Global) Stablecoins bring the payment element to distributed ledger networks. This potentially enables 24/7, real-time, "delivery-versus-payment"/"payment-versus-payment"/"delivery-versus-delivery" exchange of "digital assets" against digital cash within DLT, exceeding "delivery-versus-delivery" of assets.

The value of stablecoins, however, very much depend on the credit quality of their issuer and/or the quality and accessibility of the reserves held by the issuer ('collateral', like securities, bonds, currencies). Ideally, stablecoins should be pegged 1:1 with central bank money in only one currency and in an insolvency remote way on a private/permissioned infrastructure. Especially, for the wholesale market the quality of stablecoins must be at least like the quality of money in relevant legacy systems.

Global stablecoins could bridge ecosystems of different providers and might also be relevant for the retail sector but should be based on quality criteria that have to be fulfilled, independent of the type of the chain (permissioned/permissionless). In this sense, backed/fiat stablecoins can be used as i.e. cheap, fast and swift payment instrument and support enhanced financial inclusion.

Q13 - In your opinion, what are the most important risks related to "stablecoins"?

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

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

Q13.1 - Is there any other important risks related to "stablecoins" not mentioned above that you would foresee?

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

FESE believes legal uncertainty is an additional risk for "stablecoins" as ambiguous rights and obligations could make stablecoins arrangements vulnerable to loss of confidence with potential severe consequences for financial stability.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q13.2 - Please explain in your answer potential differences in terms of risks between "stablecoins" and "global stablecoins" (if needed).

The risks differ depending on which assets (e.g. currencies, commodities, real estate or securities) the 'stable coin' is backed by and the legal rights of its holders. Money laundering, securities trading, banking, fund management and financial infrastructure regulation can all be of relevance (to mitigate the risks).

Q14 - In your view, would a bespoke regime for crypto-assets (that are not currently covered by EU financial services legislation) enable a sustainable crypto-asset ecosystem in the EU (that could otherwise not emerge)?

☒Yes
☐No
☐Don't know / no opinion/ not relevant

Q14.1 - Please explain your reasoning (if needed).

FESE supports the creation of bespoke regime at EU level, on the condition that such a regime is limited to assets that are not considered as financial instruments (please see our answer to Q8 on "crypto tokens"). The creation of a bespoke regime for "crypto-assets" considered as financial instruments (i.e. what we consider as "investment/security tokens"), would risk creating an unlevel playing field with traditional financial instruments and come at the expense of investor protection. 'Investment/security tokens' should be considered as financial instruments under MiFID II (Article 4, paragraph 15) and no discretion should be left to Member States to change this EU interpretation at local level.

Q15 - 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.

EU countries have taken varied stances on "crypto-assets", supported by new disruptive technology. Whilst there seems to be a common acceptance that tokens can take the form of security, payment and utility, the regulations of these tokens do vary in different member states and countries generally. Please find below some national examples: In 2017, the French national competent authority (AMF) authorised the use of blockchain to register and transfer financial instruments not admitted on regulated trading venues. This was a positive development to clarify the potential use of blockchain for these instruments. In 2018, the French government adopted a legislative framework for initial coin offerings (ICOs) which are not considered as financial instruments, with an optional AMF visa for their public placement and the proper protection of investors' funds in an escrow account. Even if it is too soon to evaluate its success - one project has been approved so far in December 2019 (for the French-ICO, willing to develop a financing platform) – it provides a welcome framework to better inform and protect investors. In November 2019, the French government has also adopted an ad-hoc regime for service providers in "crypto-assets" not qualifying as financial instruments (Prestataires de Services en Actifs Numériques - PSAN), with adapted requirements applicable to distribution, brokerage, trading venues and custody services versus those applicable for

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

financial instruments. The regime notably allows trading venues to accept direct orders from end clients. About 10 projects are said to be currently examined for licensing. The overall framework is positive as it provides a certain degree of investor protection for otherwise non-regulated assets. Yet, some requirements appear questionably lighter than those applicable when the same function are performed in relation to financial instruments. For instance, trading platform operators are allowed to execute orders discretionarily, to trade on own account on the platform they operate and benefit from some leeway regarding pre- and post-trade transparency.

In November 2019, the German legislator introduced a new regulatory framework for "crypto-assets". As part of the transposition of the Fifth EU Money Laundering Directive into national law, the German legislator amended the German Banking Act (Kreditwesengesetz – KWG) to provide legal clarity regarding "crypto-assets".

As of 1st January 2020, "crypto-assets" are classified as financial instrument under the German Banking Act. Therefore, entities which provide services with respect to "crypto-assets", are required to be licensed by BaFin. This also holds for crypto-custody services.

The German legislator defines "crypto-assets" as "(…) digital representations of a value

- that has not been issued or guaranteed by any central bank or public body and does not have the legal status of currency or money,
- is accepted by natural or legal persons as a means of exchange or payment by virtue of an agreement or actual practice, or is used for investment purposes and
- can be transferred, stored and traded electronically."

E-money and monetary values within the meaning of the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz – ZAG) are expressly excluded from the scope of such defined "crypto-assets".

As explicitly laid out in the recitals (BR-Drs 352/19, p. 122), the new term of "crypto-assets" serves as a catch-all provision. Therefore, if a crypto-asset also qualifies as a security, the provisions on securities will be applied primarily. The crypto-asset specific provisions therefore will only be applied to those "crypto-assets" that do not fall into the scope of other financial instruments.

With this decision, the German legislator follows the principle "Same business, same rules", i.e. financial instruments are, in principle, regulated in a technology-neutral approach, but, to provide a holistic regulatory landscape, other "crypto-assets" that do not fall into the scope of any 'classical' financial instruments are now also included in the regulation. The incorporation of "crypto-assets" into already existing regulatory framework appears internationally to be the prevailing approach.

Q16 - 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).

Based on the French and German regimes as illustrated above, FESE sees the possibility for bespoke regimes to be developed at national level by the national relevant competent supervisory authorities for "digital-assets" that do not act as financial instruments and use cryptology (which could be defined as "crypto-tokens").

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

However, FESE is concerned that the implementation of national bespoke regimes may adversely provide regulatory alleviations to "crypto-assets" representing financial instruments using cryptology); thereby introducing legal uncertainty which puts at risk the principles provided by the EU regulatory framework which safeguards market integrity and investor protection.

For instance, under the French PSAN bespoke regime, some requirements appear questionably lighter than those applicable when the same function are performed in relation to financial instruments. For example, trading platform operators are allowed to execute orders discretionarily, to trade on own account on the platform they operate and benefit from some additional exemptions regarding pre- and post-trade transparency of "crypto-assets". For financial instruments, regulated markets and MTF are subject to requirements prohibiting these types of activities.

There is a need to maintain the same level of obligations for financial market participants trading "crypto-assets" that act as financial instruments and those trading traditional financial instruments. If not, there is a risk of introducing regulatory arbitrage based on the technology used. We believe that the creation of bespoke regimes for "crypto-assets" would inadvertently facilitate this regulatory arbitrage, at the expense of investor protection provisions guaranteed by the current legislative framework.

As a first step, it is therefore important to make a classification of "digital assets" and a categorisation of "crypto-assets" at EU level to distinguish between different forms of tokens (as suggested by the Commission), notably to make a clear differentiation between "digital-assets" that act as financial instruments based on the existing MiFID II framework and use cryptology (i.e. "crypto-assets") and "digital-assets" that do not act as a financial instruments and use cryptology (which could be defined as "crypto-tokens").

This differentiation could then allow for the creation of an EU level bespoke regime for "crypto-tokens" ("digital assets" that do not act as financial instruments) based on a set of concrete qualifications and criteria and allow for innovation in that field without compromising market integrity and investor protection in the trading of "crypto-assets".

Moreover, this clarification would allow to identify which existing provisions would have to be amended to clarify the legal framework to encourage the trading of "crypto-assets" that act as financial instruments , whilst preserving the principles of market integrity and investor protection embedded in law.
FESE advocates for incorporating a classification of "other digital-assets" in the existing European financial regulatory framework instead of creating a bespoke regulatory regime. Existing regulation should be supplemented where required to address technology related "new" risks. This would provide for legal certainty for market participants as they ensure high standards of investor protection and market integrity. This approach would create a level playing field for market participants and allow for innovation, while taking investor protection concerns seriously.

Q17 - Do you think that the use of crypto-assets in the EU would be facilitated by greater clarity as to the prudential treatment of financial institutions' exposures to crypto-assets? (See the discussion paper of the Basel Committee on Banking Supervision (BCBS))

☒Yes
☐No
☐Don't know / no opinion/not relevant

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q17.1 - Please explain your reasoning for your answer to question 17:

As referred above, FESE supports an EU-level bespoke regime for tokens that are not considered as financial instruments under MiFID II, as modelled by the French PSAN regime to non-financial "crypto-assets" (which could be defined as "crypto-tokens"). As stated, the category of 'investment/security token' may be used to define "crypto-assets" that are considered as financial instruments under MiFID II/MiFIR. Clarity should also be provided regarding the prudential treatment of financial institutions´ exposures to "digital assets", aligned with BIS/Basel Committee.

Q18 - 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?

Binding EU provisions on the transfer of digital-assets and digitalisation of tangible assets would greatly help achieving an EU market in respect of a token-based economy. This would solve the issues of the applicable law regarding content and requirements. Please refer also to the IOSCO report "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms".

Q19 - 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?

N/A

1. Issuance of crypto-assets in general

Q20 - Do you consider that the issuer or sponsor of crypto-assets marketed to EU investors/consumers should be established or have a physical presence in the EU?

☐Yes
☒No
☐Don't know / no opinion/not relevant

Q20.1 - Please explain your reasoning (if needed).

The issuer or sponsor of "crypto-assets" marketed to EU investors/consumers should not have an obligation to be established or have a physical presence in the EU. Third country issuers or sponsors can access the EU "crypto-assets" market in respect of existing EU regulatory framework and principles provided to them. A physical presence of issuers and sponsors of digital-assets marketed to EU investors is not necessary, if "digital-assets" are covered by the definition of financial instruments and financial services, as EU equivalence rules would apply or national competencies would ensure investor protection.

Q21 - Should an issuer or a sponsor of crypto-assets be required to provide information (e.g. through a 'white paper') when issuing crypto-assets?

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q21.1 - Please indicate the entity that, in your view, should be responsible for this disclosure (e.g. the issuer/sponsor, the entity placing the crypto-assets in the market) and the content of such information (e.g. information on the crypto- asset issuer, the project, the rights attached to the crypto-assets, on the secondary trading, the underlying technology, potential conflicts of interest…).

On a general level, it is crucial to require a standardised information set from issuers or sponsors of "digital-assets", which informs the public about the "crypto-asset" based on specified criteria. However, it needs to be acknowledged that not every "digital-asset" has an identifiable issuer or sponsor. Any group of actors that are involved in the public offering of these assets need to inform potential investors. This should be achieved by having a requirement to publish a respective risk profile and additional information on the rights and risks that are embedded in such an offering. An issuer or provider of a 'security/ investment token' available for retail investor should provide the same level of information to investors as any other equivalent financial instruments. It is up to the NCAs to define and provide issuers, service providers or operators with the appropriate regime for transparency and prospectus. The level of information to investors might be lighter for certain groups (e.g. SMEs Growth Markets or certain types of bonds) but the level of disclosure should not be linked with the product being a tokenised product or not.

Q22 - If a requirement to provide the information on the offers of crypto-assets is imposed on their issuer/sponsor, would you see a need to clarify the interaction with existing pieces of legislation that lay down information requirements (to the extent that those rules apply to the offers of certain crypto-assets, such as utility and/or payment tokens)? Please rate each proposal from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
The Consumer Rights Directive						
The E-Commerce Directive						
The EU Distance Marketing of Consumer Financial Services Directive						

Q22.1 - Is there any other existing piece of legislation laying down information requirements with which the interaction would need to be clarified?

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

N/A

Q22.2 - Please explain your reasoning and indicate the type of clarification (legislative/non legislative) that would be required.

N/A

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q23 - Beyond any potential obligation as regards the mandatory incorporation and the disclosure of information on the offer, should the crypto-asset issuer or sponsor be subject to other requirements?

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

	1	2	3	4	5	No opinion
The managers of the issuer or sponsor should be subject to fitness and probity standards						
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						

Q23.1 - Is there any other requirement not mentioned above to which the crypto-asset issuer should be subject?

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

N/A

Q23.2 - Please explain your reasoning for your answer to question 23:

N/A

Q24 - In your opinion, what would be the objective criteria allowing for a distinction between "stablecoins" and "global stablecoins" (e.g. number and value of "stablecoins" in circulation, size of the reserve…)? Please explain your reasoning.

FESE would suggest aligning the criteria with international standard setters, i.e. IOSCO.

Q25.1 - To tackle the specific risks created by "stablecoins" and "global stablecoins", what are the requirements that could be imposed on their issuers and/or the manager of the reserve?

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

	"Stablecoins"		
	Relevant	**Not relevant**	**Don' know/no opinion/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			

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q25.1 - a) Is there any other requirements not mentioned above that could be imposed on "stablecoins" issuers and/or the manager of the reserve?

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

FESE would propose the following criteria to distinguish stablecoins from global stablecoins: (i) number of currencies included (coin itself and/or reserve pool), (ii) number of participants and (iii) volumes of coins issued as well as (iv) the underlying assets´ insolvency regimes. To address the mentioned risks, the issuer and/or system operator should ideally be authorised and supervised. A strong rulebook (either from the regulator and/or from the system operator) should be required including measures that define the rules of a passive management of the reserve (e.g. fiat-money only, no cross-currency risk etc.) Additional requirements for the issuer and/or manager of the reserve should be: Assets of the reserve should be kept at a central bank or regulated/supervised institutions; assets of the reserve should be highly liquid, with limited market and credit risk; prudent risk parameters should be applied for the reserve; e.g. composition of reserve (cash vs. securities), concentration risks, definition of volume caps per currency, ratios of asset classes amongst each other. If reserves are in cash, then these should ideally be held with central banks; if with commercial banks, then risk diversification would be required i.e. limited amount per bank. To address specific risks of stablecoins and global stablecoins a limitation in the geographical spread through underlying regional networks might be helpful. As this is a fast-evolving field, it is important to take a prudent approach in addressing these issues.

Q25.1 - b) Please illustrate your response for "Stablecoins" (if needed).

N/A

Q25.2 - To tackle the specific risks created by "stablecoins" and "global stablecoins", what are the requirements that could be imposed on their issuers and/or the manager of the reserve?

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

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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			

Q25.2 - a) Is there any other requirements not mentioned above that could be imposed on "global stablecoins" issuers and/or the manager of the reserve?

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

N/A

Q25.2 - b) Please illustrate your response for "Global Stablecoins" (if needed).

N/A

Q26 - Do you consider that wholesale "stablecoins" (those limited to financial institutions or selected clients of financial institutions, as opposed to retail investors or consumers) should receive a different regulatory treatment than retail "stablecoins"?

☒Yes

☐No

☐Don't know / no opinion/not relevant

Q26.1 - Please explain your reasoning (if needed).

It makes sense to differentiate between wholesale and retail clients. The end customer (retail investor, consumer) needs a higher level of protection than a professional investor (financial institution or selected client of a financial institution).

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Trading platforms

Q27 - In your opinion and beyond market integrity risks (see section III. C. 1. below), what are the main risks in relation to trading platforms of crypto-assets?

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

	1	2	3	4	5	No opinion
Absence of accountable entity in the EU				X		
Lack of adequate governance arrangements, including operational resilience and ICT security				X		
Absence or inadequate segregation of assets held on the behalf of clients (e.g. for 'centralised platforms')				X		
Conflicts of interest arising from other activities				X		
Absence/inadequate recordkeeping of transactions				X		
Absence/inadequate complaints or redress procedures are in place				X		
Bankruptcy of the trading platform				X		
Lacks of resources to effectively conduct its activities				X		
Losses of users' crypto-assets through theft or hacking (cyber risks)				X		
Lack of procedures to ensure fair and orderly trading				X		
Access to the trading platform is not provided in an undiscriminating way				X		
Delays in the processing of transactions				X		
For centralised platforms: Transaction settlement happens in the book of the platform and not necessarily recorded on DLT. In those cases, confirmation that the transfer of ownership is complete lies with the platform only (counterparty risk for investors vis-à-vis the platform)				X		
Lack of rules, surveillance and enforcement mechanisms to deter potential market abuse				X		

Q27.1 - Is there any other main risks posed by trading platforms of crypto-assets not mentioned above that you would foresee?

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

FESE would like to highlight the importance of distinguishing between different types of "crypto-assets" and allow for 'investment/security tokens' to be recognised as financial instruments under MiFID II. Crypto-asset trading platforms could then be considered as regulated, secure and transparent as traditional trading venues for both issuers and investors.

In the absence of such classification, categorisation and definition, we believe a clear regulatory distinction should be made between non-financial instruments that use cryptology and financial instruments that use cryptology, where the latter would be subject to MiFID II/MiFIR.

More specifically, any asset deemed as a financial instrument should be traded only on trading venues as defined in MiFID II, i.e. regulated markets, MTFs or OTFs. For trading platforms, price formation in multilateral trading and price dissemination should be ensured, enabling investors to find a price orientation that meets regulatory standards.

Regulation should ensure that there is no difference between trading against fiat money or trading against other regulatory-compliant "digital-assets" (for example due diligence check, public-address check, etc.).

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Price formation needs to follow proper rules and should have an appropriate level of pre- and post-trade transparency. Eventual exemptions and waivers could be granted by ESMA.

Q27.2 – Please explain your reasoning (if needed).

Regarding the main risks in relation to trading platforms for "crypto-assets", this strongly depends on the type of "crypto-asset", the governance structure (i.e. centralised vs. decentralised, permissioned vs. non permissioned access) and the underlying technology. Trading platforms who operate trading in "crypto-assets", which are classified as 'investment/security' tokens, should follow established financial market rules.

In the absence of such classification, FESE wishes to make remarks on the main risks related to these 'investment/security token'-platforms:

- **Absence of accountable entity in the EU**: or in a recognised third country, will prove to be a clear risk for a platform, notably for dispute resolutions.
- **Absence or inadequate segregation of assets held on the behalf of clients (e.g. for 'centralised platforms'):** There are real loss-risks for investors, notably due to thefts as illustrated recently by the $190m stolen on QuadrigaCX or the $16m stolen on Cryptopia.
- **Conflicts of interest arising from other activities:** Most "crypto asset"-trading platforms combine potentially conflicting activities: (i) operation of a trading venue, (ii) reception / transmission of client orders on the platform, (iii) trading on own account and (iv) custody of clients' assets and cash.
- **Absence/inadequate recordkeeping of transactions:** This risk is particularly relevant in the case of centralised platforms, where transactions - before being sent on the blockchain - are intermediated by the operator, who may therefore send the recordkeeping of transactions in batches rather than individually.
- **Absence/inadequate complaints or redress procedures are in place:** Today the procedures rely on the willingness of each platform. There are auto-regulated mechanisms in place – such as within the Virtual Commodity Association, the Blockchain Association, or Japan Virtual Currency Exchange Association - but a more harmonised approach, at least for entities active with EU customers, would be welcome.
- **Bankruptcy of the trading platform:** This is especially problematic when the platform also acts as a custodian and as an intermediary for the transactions of the clients - as illustrated by Cryptopia - resulting in losses for investors. When the platform does not act as a custodian, nor intermediate transactions, the risk is a lot more limited particularly whilst considering the relative fragmentation of the crypto-asset market.
- **Losses of users' "crypto-assets" through theft or hacking (cyber risks):** This risk has materialised several times, including amongst the largest platforms such as Binance, where $40m were lost in May 2019. Whilst the most serious and equipped platforms pay back clients, this is detrimental to the overall market, as it undermines trust.
- **Lack of procedures to ensure fair and orderly trading:** This is especially problematic considering the fact that many "crypto-asset"- trading platforms combine conflicting activities, thereby threatening the fair and orderly trading process.
- **Access to the trading platform is not provided in an undiscriminating way:** This is especially problematic as the platform may have an interest in filtering flows when trading on account for instance.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q28 - What are the requirements that could be imposed on trading platforms in order to mitigate those risks? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

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

Q28.1 - 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:

Another issue is that "crypto-assets"-trading platforms currently do not comply with requirements in relation to the organisation of secondary markets. FESE considers that all such platforms should be regulated as regulated markets, MTFs or OTFs under MiFID II/MiFIR. Intermediaries should be held responsible in order to prevent conflict of interest, money laundering, financing of terrorism etc.

Q28.2 - 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:

The requirements that could be imposed on trading platforms to mitigate risks, strongly depend on the type of "crypto-asset" traded, the governance structure and the underlying technology. Trading platforms who operate trading in "crypto-assets" classified as 'investment/security tokens', should follow established financial market rules, thereby mitigating the risks. Segregation of asset (classified as 'investment/security tokens') or AML requirements should be tackled within post trading infrastructures.

We would consider that:

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

- Trading platforms should have a physical presence in the EU: or have a physical presence in recognised 3rd countries.
- Trading platforms should be subject to prudential requirements (including capital requirements): This should take into account other activities they may undertake (in particular custody / intermediation of client transactions).
- Trading platforms should have adequate rules to ensure fair and orderly trading: The rules regarding pre- and post-trade transparency, non-discretionary execution, non-discriminatory access and prevention against conflicts of interests should be the same as for trading venues for financial instruments.
- Trading platforms should be responsible for screening "crypto-assets" against the risk of fraud: or rely on assets that have been approved by recognised regulators

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

Q29 - In your opinion, what are the main risks in relation to crypto-to-crypto and fiat- to-crypto exchanges? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

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

Q29.1 - Is there any other main risks in relation to crypto-to-crypto and fiat-to-crypto exchanges not mentioned above that you would foresee?

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

While the word 'Exchange' is not formally defined in legislation, FESE would like to underline that it is commonly used to refer to regulated markets and other trading venues as defined in MiFID II/MiFIR.

Considering that the types of "crypto-asset"-trading platforms described above do not fulfil requirements applicable to trading venues, it is important not to create ambiguities in terms of the language used to describe these, as calling them exchanges may wrongly create the impression that these are regulated entities subject to, inter alia, investor protection requirements.

In other words, these "crypto-assets"-trading platforms should have to follow the same rules applicable to trading venues (e.g. accountability, operational resilience / ICT security, recordkeeping). In order to apply all benefits to all types of trading of financial instruments no differentiation between crypto to crypto vs. crypto to fiat should be made. All market participants should act with a respective authorisation and/or set of licenses

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

according to their activities/services (e.g. payment, execution of security transactions at an MTF, safe keeping of digital-assets, safekeeping of securities, organising a multilateral trading facility etc.).

Q29.2 - Please explain your reasoning for your answer to question 29:

- **Absence of accountable entity in the EU:** in order to apply relevant requirements to "crypto asset"-trading platforms and protect EU investors, it would be necessary for platforms selling services to EU investors to have an accountable entity in the EU or in a recognised third country
- **Lack of adequate governance arrangements, including operational resilience and ICT security:** Similarly to exchanges that trade standard financial instruments, "crypto-asset"-trading platforms must have proper governance arrangements, including on operational resilience and ICT in order to limit risks for investors. More specifically, when the platform also acts as a custodian on behalf of its clients (even on a temporary basis), specific requirements should be established to prevent hacks and thefts of wallets with proper cybersecurity standards and clear and transparent rules regarding the conditions under which the clients' assets will be guaranteed by the "crypto-asset"-trading platform in case of such security breaches.
- **Conflicts of interest arising from other activities:** Most "crypto-asset"-trading platforms currently combine potentially conflicting activities. Depending on the scale of these activities, two possible approaches would help prevent potential threats to investor protection and market integrity:
  - **Option 1:** Requiring platforms to properly disclose conflict of interest risks to clients and potential clients, and to have in place proper governance arrangements to limit these associated risks. For instance, different entities should be required to have Chinese Walls in place (virtual barrier intended to block the exchange of information between departments to prevent conflicts of interest) for each conflicting activities such as exchange operations, reception and transmission of client orders, trading on own account and custody services (even when done on a temporary basis). Additionally, if the "crypto-asset"-trading platform is acting as a receptor-transmitter of client orders, the "crypto-asset"-trading platform should be required to route client orders and execute them in a non-discretionary manner.
  - **Option 2:** "Crypto asset"-trading platforms could be prevented from combining conflicting activities. Similar to trading venues for standard financial instruments, the platform (or its holding entity) should be prevented from trading on own account on the platform they operate. Additionally, when acting as custodians, platforms should be prevented from using the assets held on custody on behalf of their clients.
- **Absence/inadequate recordkeeping of transactions:** in order to be able to investigate potential market abuses, "crypto-asset"-trading platforms should be required to properly record transactions, in the same manner as trading venues for standard instruments.
- **Absence/inadequate complaints or redress procedures are in place:** platforms should have clear, transparent and non-discretionary complaint or redress procedures to provide investors with a safe and predictable trading environment in this respect and hence foster investor trust.
- **Bankruptcy:** a first step to prevent risks of losses for investors would be to require platforms that conduct activities linked to custody to have procedures and/ or sufficient funds in place to guarantee their clients' assets in case of a bankruptcy.
- **Losses of users' "crypto-assets" through theft or hacking:** please see our answers above on the risks related to the lack of adequate governance arrangements, including operational resilience and ICT security, conflicts of interest arising from other activities and inadequate own funds to repay the consumers.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

- **Users suffer loss when the platform they interact with does not exchange "crypto-assets" against fiat currency (conversion risk):** platforms providing crypto to crypto trading should be required to provide clients with proper information about the types of "crypto-assets" involved on their operating platforms, including their volatility profile and any related conversion risk.
- **Absence of transparent information on the "crypto-assets" proposed for exchange:** platforms should provide clients and prospective clients with clear information on the "crypto-assets" they provide, notably regarding their level of volatility, the issuing entity (its location and project), the types of rights allocated to clients holding these assets and potential conflicts of interests when the platform is the issuer of the asset or has invested in it.

Q30 - What are the requirements that could be imposed on exchanges in order to mitigate those risks?

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

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

Q30.1 - Is there any other requirement that could be imposed exchanges in order to mitigate those risks?

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

While the word 'Exchange' is not formally defined in legislation, FESE would like to underline that it is commonly used to refer to regulated markets and other trading venues as defined in MiFID II/MiFIR.

Considering that the types of "crypto-asset"-trading platforms described above do not fulfil requirements applicable to trading venues, it is important not to create ambiguities in terms of the language used to describe these, as calling them exchanges may wrongly create the impression that these are regulated entities subject to, inter alia, investor protection requirements.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q30.2 - Please indicate if those requirements should be different depending on the type of crypto-assets available on the exchange and explain your reasoning (if needed).

Generally, the requirements should be applied to all types of assets.

- **"Crypto-asset"-trading platforms should be responsible for screening "crypto-assets" against the risk of fraud:** an alternative would be to require platforms to properly disclose that the asset they propose for trading has not (or could not) be screened for risks of fraud.
- For all other requirements, please refer to the answers given above (question 29.1).

Provision of custodial wallet services for crypto-assets

Q31 - In your opinion, what are the main risks in relation to the custodial wallet service provision? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

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

Q31.1 - 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:

It should not be allowed to transfer "digital-assets", including digital money, from and to anonymous accounts without any onboarding or Know Your Customer (KYC) requirements. Wallet provider should be regulated and falling under the AML, to create trust in the digital and crypto market. Further guidance on AML/KYC handling of accidental/unintended transfers is also needed, given the irreversibility of transactions especially on public chains.
There is legal uncertainty with respect to the allocation of ownership as regards the holdings in a wallet, if this is not provided for by law (holders of private keys could qualify as quasi-owners of the relevant tokens, but this would not be appropriate for a multi-level holding custody structure).

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

It should also be clarified under which conditions material outsourcing with regard to "digital asset"-custody would be allowed (e.g. counterparty risk, standards, IT security etc.).To ensure the integrity of the financial markets and mitigate risks, custodial wallet providers for the provision of custody are obliged entities and have to comply with the fifth AMLD. In addition, these should be licensed as financial service providers.

Q31.2 - Please explain your reasoning (if needed).

For third country firms offering services to EU citizens, the existence or non-existence of a physical presence in the EU does not constitute per se a risk to EU investors. The level of risk depends on the nature of services and products offered and the type of investor.

FESE would propose the following definition of "custodian wallet provider": "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer cryptographical and other digital assets.".

Q32 - What are the requirements that could be imposed on custodial wallet providers in order to mitigate those risks? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

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

Q32.1 - 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:

The requirements defined in the French "PSAN regime", detailed in the AMF rulebook (Book VII, Title II Section 1) should be replicated at European level.

Proper recording of any impactful event: any events that can have an impact on the clients' rights attached to the assets (fork for instance) should be properly recorded by the custodian.

Outsourcing: the custodial service provider can outsource part (but not all) of the services to a third party provided this party complies with the requirements applicable to these

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

services. In all cases, the custodial service providers remain solely responsible for the duties it owns vis à vis its clients.

Reporting: the custodial service provider should have reporting obligations, at least once every quarter of the year, to its clients on their holdings and movements on their accounts.

Contract: before providing any services, the custodial service provider should have a contract in place with the client.

Access: The custodial service provider should define, in a transparent and objective way, the types of clients to whom it agrees to provide its services and apply these criteria in a non-discretionary way.

Furthermore, custodians and CSDs should be allowed (according to CSDR) to hold any kind of "digital asset" in appropriate custody systems. There has to be clarity regarding when "crypto-assets" are compliant with AMLD. Since digital utility assets may evolve into digital hybrid-securities, at any given time, all kinds of "digital assets" should be "custodiseable" within a CSD or custodian bank.

Q32.2 - Please indicate if those requirements should be different depending on the type of crypto-assets kept in custody by the custodial wallet provider and explain your reasoning for your answer to question 32:

Generally, the requirements should be applied to all types of assets.

The requirements defined in the French "PSAN regime", detailed in the AMF rulebook (Book VII, Title II Section 1) should be replicated at European level.

Q33 - Should custodial wallet providers be authorised to ensure the custody of all crypto-assets, including those that qualify as financial instruments under MiFID II (the so-called 'security tokens', see section IV of the public consultation) and those currently falling outside the scope of EU legislation?

☒Yes

☐No

☐Don't know / no opinion/not relevant

Q33.1 - Please explain your reasoning for your answer to question 33:

Yes, provided that custodial wallet providers are compliant with all applicable rules regarding custody of financial instruments.

Q34 - 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?

FESE would advise to regulate custodial wallet providers as regulated entities in order to ease the regulatory process.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Other service providers

Q35 - 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 each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

	1	2	3	4	5	No opinion
Reception and transmission of orders in relation to crypto-assets				X		
Execution of orders on crypto-assets on behalf of clients				X		
Crypto-assets portfolio management				X		
Advice on the acquisition of crypto-assets				X		
Underwriting of crypto-assets on a firm commitment basis				X		
Placing crypto-assets on a firm commitment basis				X		
Placing crypto-assets without a firm commitment basis				X		
Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets)				X		
Processing services, also known as 'mining' or 'validating' services in a DLT environment (e.g. 'miners' or validating 'nodes' constantly work on verifying and confirming transactions)				X		
Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers)				X		
Services provided by developers that are responsible for maintaining/updating the underlying protocol			X			
Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with)			X			

Q35.1 - 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:

Further requirements are needed for services which are similar to those already regulated on EU level (e.g. by Annex I A of MiFID II), including the 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 (or services defined in CSDR, EMIR or AIFMD).

Q35.2 - Please illustrate your response, by underlining the potential risks raised by these services if they were left unregulated and by identifying potential requirements for those service providers.

Reception and transmission of orders in relation to "crypto-assets": These activities should be subject to requirements, as the absence of regulation would risk the reception and transmission to be discretionary, resulting in potentially detrimental results in terms

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

of execution quality for investors. Absence of regulatory requirements would also invite conflicts of interest within entities which performs both reception and transmission of orders and trading on own account.

Execution of orders of "crypto-assets" on behalf of clients: same as above.

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) and services provided by developers that are responsible for maintaining/updating the underlying protocol: Today, even for standard financial instruments, there is no specific framework for pure technical operators. The requirements apply to functional operators. The challenge regarding the adoption of a framework applicable to a blockchain environment is precisely that the goal of this technology is to replace the role of the former functional operator by a purely decentralised technology. The absence of any requirements applicable to this technological layer would result in operational and systemic risks. A solution would be either to subject miners themselves to a dedicated set of requirements or have requirements for entities operating the related protocols which would then be specific to miners and developers.

Q36 - Should the activity of making payment transactions with crypto-assets (those which do not qualify as e-money) be subject to the same or equivalent rules as those currently contained in PSD2?

☐Yes
☐No
☐Partially
☒Don't know/no opinion/not relevant

Q36.1 - Please explain your reasoning for your answer to question 36:

N/A

C. Horizontal questions

Q37 - In your opinion, what are the biggest market integrity risks related to the trading of crypto-assets?

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

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

Q37.1 - 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:

The horizontal issues market integrity, AML/countering financing of terrorism, consumer/ investor protection, as well as supervision and oversight of "digital-assets" service

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

providers are very important to make the new asset class trustworthy, secure and successful.
The more effectively those issues are addressed, the easier (institutional) investors could invest and help the market to develop (bringing size, liquidity, professionalism).
It would be advisable to bring the "digital-asset" ecosystem to the same level of regulation as other asset classes.
Regarding investor protection:

- Investor protection rules are appropriate for "digital-assets". Potential amendments of such rules as a result of the MiFID Review should consider specific risks attached to "digital-assets".
- To realise the potential of the new asset class, the usual rules should apply in general, but if necessary, additional IT related requirements shall also apply (e.g. safeguarding the integrity of a DLT-network).

Q37.2 - Please explain your reasoning for your answer to question 37:

If trading of "crypto-asset" continues on platforms not subject to financial market regulations i.e. MiFIDII/MiFIR nor the Market Abuse Regulation, it should be noted that all of the above options would pose significant risks.

Q38 - In your view, how should market integrity on crypto-asset markets be ensured?

Another issue related to "crypto-assets" in the context of trading, is the applicability of requirements in relation to the organisation of secondary markets where these are traded. FESE considers that all such platforms should be regulated as regulated markets, MTFs or OTFs under MiFID II/MiFIR.

Q39 - Do you see the need for supervisors to be able to formally identify the parties to transactions in crypto-assets?

☒Yes
☐No
☐Don't know / no opinion/not relevant

Q39.1 - Please explain your reasoning (if needed). If yes, please explain how you would see this best achieved in practice.

N/A

Q40 - 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?

While the word 'Exchange' is not formally defined in EU legislation, FESE would like to underline that it is commonly used to refer to regulated markets and other trading venues as defined in MiFID/MiFIR.

Considering that the types of platform described above do not fulfil requirements applicable to trading venues, it is important not to create ambiguities in terms of the language used to describe these, as calling them exchanges may wrongly create the impression that these are regulated entities subject to, inter alia, investor protection requirements.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q41 - Do you consider it appropriate to extend the existing 'virtual currency' definition in the EU AML/CFT legal framework in order to align it with a broader definition (as the one provided by the FATF or as the definition of 'crypto- assets' that could be used in a potential bespoke regulation on crypto-assets)?

☒Yes
☐No
☐Don't know / no opinion/not relevant

Q41.1 - Please explain your reasoning (if needed).

FESE would recommend any appropriate opportunity to align definitions with those operated by international standard setting bodies, such as the FATF. Harmonising language and definitions are core to the delivery of better regulatory outcomes and enabling a safe and efficient global trading environment.

Q42 - 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.

☒Yes
☐No
☐Don't know / no opinion/not relevant

Q42.1 - Please explain your reasoning for your answer to question 42:

Any "crypto-asset"-trading platform operating as an exchange or that is able to provide trading venue or Financial Market Infrastructure services, especially those available to retail investors, should confirm and abide by the AML/CFT regulatory requirements imposed on traditional market infrastructures.

Q43 - If a bespoke framework on crypto-assets is needed, do you consider that all crypto-asset service providers covered by this potential framework should become 'obliged entities' under the EU AML/CFT framework?

☒Yes
☐No
☐Don't know / no opinion/not relevant

Q43.1 - Please explain your reasoning for your answer to question 43:

Please see our response under question 42.1

Q44 - 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?

N/A

Q45 - Do you consider that these requirements should be introduced in the EU AML/CFT legal framework with additional details on their practical implementation?

☐Yes
☐No

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

☐Don't know / no opinion/not relevant

Q45.1 - Please explain your reasoning (if needed).

N/A

Q46 - In your view, do you consider relevant that the following requirements are imposed as conditions for the registration and licensing of providers of services related to crypto-assets included in section III. B? Please rate each proposal by level of relevance from 1 to 5, 1 standing for "completely irrelevant" and 5 for "highly relevant".

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

Q46.1 - Please explain your reasoning for your answer to question 46:

N/A

Q47 - What type of consumer protection measures could be taken as regards crypto- assets?

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

	1	2	3	4	5	No opinion
Information provided by the issuer of crypto-assets (the so-called 'white papers')						
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…)						

Q47.1 - Is there any other type of consumer protection measures that could be taken as regards crypto-assets?

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

N/A

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q47.2 - Please explain your reasoning and indicate if those requirements should apply to all types of crypto assets or only to some of them.:

N/A

Q48 - Should different standards of consumer/investor protection be applied to the various categories of crypto-assets depending on their prevalent economic (i.e. payment tokens, stablecoins, utility tokens…) or social function?

☐Yes
☐No
☐Don't know / no opinion

Q48.1 - Please explain your reasoning for your answer to question 48.

N/A

Q49 - Should different standards in terms of consumer/investor protection be applied depending on whether the crypto-assets are bought in a public sale or in a private sale?

☐Yes
☐No
☐Don't know / no opinion

Q49.1 - Please explain your reasoning for your answer to question 49.

N/A

Q50 - Should different standards in terms of consumer/investor protection be applied depending on whether the crypto-assets are obtained against payment or for free (e.g. air drops)?

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

Q50.1 - Please explain your reasoning for your answer to question 50:

N/A

Q51 - In your opinion, how should the crypto-assets issued in third countries and that would not comply with EU requirements be treated?

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

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q51.1 - Is there any other way the crypto-assets issued in third countries and that would not comply with EU requirements should be treated?

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

N/A

Q51.2 - Please explain your reasoning for your answer to question 51:

In order to enable cross-border trade, appropriate measures should be taken to ensure that such products can be traded with recognised third countries.

Q52 - 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).

Any crypto-asset service provider which operates/provides the services of market infrastructures should be subject to the supervision of the jurisdictions' regulatory authorities.

Q53 - Which are the tools that EU regulators would need to adequately supervise the crypto-asset service providers and their underlying technologies?

N/A

Crypto-assets that are currently covered by EU legislation

Q54 - Please highlight any recent market developments (such as issuance of security tokens, development or registration of trading venues for security tokens…) as regards security tokens (at EU or national level)?

N/A

Q55 - Do you think that DLT could be used to introduce efficiencies or other benefits in the trading, post-trade or asset management areas?

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

Q55.1 - Please explain your reasoning for your answer to question 55:

Combining innovative technologies, for instance blockchain based technologies, with established, highly regulated market infrastructures would be the natural choice in order to ensure market stability while making use of the innovative potential brought about through FinTech. DLT has the potential to accelerate, decentralise, automate and standardise data-driven processes and therefore to alter the way in which assets are transferred and records are kept. DLT allows cross-verification of information in a transparent and dependable way and can simplify complex verification and validation processes.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Hurdles to wide scale adoption of DLT in securities markets are technical limitations, contextual aspects such as for example business model/market model design, technical integration/transition and legal/regulatory complexity.

For solutions based on DLT to reach actual implementation in securities market, visions for the future need to be broken down into defined descriptions of services and solutions that not only are accepted and desired by its intended consumers but also meet legal, regulatory and technical requirements. DLT is not a panacea that will replace all existing infrastructure in securities markets.

DLT solutions need to be integrated into the existing ecosystem of infrastructure in securities market, which will require some effort and time. Transition planning and execution is also important in DLT business cases when the intention is for DLT to replace legacy technology.

It is worth noting that a few CSDs already use DLT as part of the internal CSD core system, namely for small volumes where this solution can be rolled out in a way that limits the reconciliation needs, thereby providing more efficiency.

Q56 - Do you think that the use of DLT for the trading and post-trading of financial instruments poses more financial stability risks when compared to the traditional trading and post-trade architecture?

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

Q56.1 - Please explain your reasoning for your answer to question 56:

There is no reason to believe the technology would systematically lead to more financial stability risk in the financial ecosystem, if the following conditions apply:

- the DLT is tailored to the areas where it is proven to provide actual benefits

- the underlying principles of the legislation apply

- the necessary regulatory clarifications are provided ahead of the use of DLT in production

However, the migration from traditional trading architecture to the use of DLT, either via a whole encompassing approach or through a technological co-existence of DLT-based solutions and non DLT-based ones, may be well evaluated, namely in what relates to the possibility to increase financial stability risks. On the one hand, not all financial market players may be willing or ready to migrate to the use of DLT and, on the other, maintaining two chains would imply reconciliations that could concretely result in errors (for instance, in respect to the registry function).

Q57 - 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.

CCPs and CSDs

FESE considers that DLT will not significantly impact the role and operations of post-trade financial market infrastructure (CCPs and CSDs) roles in the near future. Post-trade market infrastructures remain relevant and are well-placed to service "crypto-assets".

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

In the context of the harmonised implementation of the CSDR, CSDs are well-placed entities to become the network service providers for "crypto-assets." Many of the functions CSDs perform would remain relevant, even though the technology currently used by CSDs is different. It would, therefore, be necessary to have clarity on the applicability of the Annex of CSDR for the provision services related to "crypto-assets".

Another aspect that should be considered relates to the risk profile of the CSDs, which should not be aggravated by servicing of "crypto-assets".

Trading venues

DLT technology has come a long way in recent years and some of the privacy and scalability issues have been resolved for its use in the capital markets industry. However, for a massive adoption of the DLT technology across the entire value chain, other critical factors need to be considered in addition to the purely technical ones. The rethinking and redesigning of the processes for a new operating model towards a decentralised solution requires not only the acceptance of all those involved in the process but also the fulfilment of legal and regulatory requirements.

FESE would rather suggest for a slow and gradual technology adoption process, therefore assuming that both solutions (traditional infrastructures and new decentralised infrastructures) will have to coexist. In recent years, processes have been improved with the use of technology and we believe that this will be the trend in the coming years. For a use of technology on the core functions of the infrastructures, FESE's view is that it will not take place in the immediate future.

Overall, DLT is not expected to fundamentally impact the role of trading venues, as the decentralised nature of this technology makes it ill-suited to create an effective price formation mechanism.

Q58 - Do you agree that a gradual regulatory approach in the areas of trading, post- trading and asset management concerning security tokens (e.g. provide regulatory guidance or legal clarification first regarding permissioned centralised solutions) would be appropriate?

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

Q58.1 - Please explain your reasoning (if needed).

FESE believes the scope of existing regulation should be sufficient to extend to most potential DLT use-cases (which are typically new technologies as opposed to new activities). Legislation, rules and supervisory practises should only be adapted if strictly required and conferring undue advantage to one technology over another or inadvertently limiting competition by unnecessarily increasing barriers to entry should be avoided.

Authorities should continue to proactively engage with industry players to identify the nature of the application, understand the technology behind it, and ensure an appropriate regulatory framework. A gradual adaptation of regulation in the would be preferable to avoid potentially drawing investors out of regulated venues into dark spaces, deeply affecting soundness and transparency of markets.

As mentioned before, FESE sees a potential risk where non-financial, unregulated firms lead developments of DLT solutions related to core market functions. A lack of awareness

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

of the regulatory environment and different risk culture may result in negative consequences for investor protection, and secure and orderly markets.

A regulatory guidance would be welcomed in order to achieve greater legal certainty and clarity for the elaboration and implementation of innovative projects within the existing regulatory framework. However, the Commission should first analyse the specific different characteristics of "crypto-assets" and ensure that a definition be made for 'investment / security tokens' to be considered as financial instruments under MiFID II, avoiding any risks of financial regulatory arbitrage based on the technology used.

MiFID II

1.1. Financial Instruments

Q59 - Do you think that the absence of a common approach on when a security token constitutes a financial instrument is an impediment to the effective development of security tokens?

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

Q59.1 - Please explain your reasoning for your answer to question 59:

FESE considers that it is important to establish key principles upon which the EU can build a role in facilitating the development and implementation of FinTech in general. These principles include, but are not limited to, the need for the application of the same rules for the same services and risks (including across different pieces of legislation) based on the principle of technology neutrality (e.g. if a 'security token' qualifies as a financial instrument, then all applicable rules within EU regulation should apply.

Therefore, the 'security token' referred to by the Commission in this question should be defined in a manner that is consistent with the definition of financial instruments under MiFID II (Article 4, paragraph 15). Once defined and submitted to proper regulations, the participants and providers of the 'investment/security token' platform will be able to act in a regulated environment. "Hybrid Tokens" (by which users may benefit also from non-financial/ non-banking items or services) should not be used to create "shadow" financial instrument with less protection for investors. The definition should be elaborated to avoid this. It is important for 'hybrid tokens' to be traded separately from security tokens.

Digital securities only become attractive for institutional investors when the associated risks are addressed in the regulatory and legal framework which builds the basis for a stable environment. The lack of certainty over the legal requirements and tax treatment applicable to security tokens is deterring issuers, investors and service providers in this area, due to the resulting risks.

Finally, it is important to clarify that where assets qualify as financial instrument (according to the MiFID II definition of financial instruments in Section C of MiFID II) they are already subject to the existing rules.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q60 - If you consider that the absence of a common approach on when a security token constitutes a financial instruments is an impediment, what would be the best remedies according to you?

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

	1	2	3	4	5	Don't know/ no opinion/not relevant
Harmonise the definition of certain types of financial instruments in the EU				X		
Provide a definition of a security token at EU level				X		
Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as security token				X		

Q60.1 - Is there any other solution that would be the best remedies according to you?

N/A

Q60.2 - Please explain your reasoning for your answer to question 60:

A harmonised definition of certain types of financial instruments would be helpful, especially for those financial instruments that can be considered security tokens. This approach could prevent a divergent response among the several jurisdictions in the EU. According to different supervisors, a security token is "any token whose value could be variable on expectancy of a future increase of loss of its valuation". That definition is widely open and a more specific definition could probably be helpful for the sake of convergence in European legislation. FESE understands the difficulty in regulating a harmonised definition for security tokens. In this regard, the efforts made by the SEC on the application of the Howey Test to securities could be an interesting example and inspiration for the regulation of any potential definition. Any definition or approach should be mindful of international efforts to harmonise the definition and have suitable flexibility to adhere to those global definitions as they come into play. However, moving towards a more harmonised approach and to have a definition at EU level would be beneficial. FESE supports further harmonising the definition of financial instrument at EU level and consider that 'investment/security tokens' should be financial instruments under MiFID II (Article 4, paragraph 15).

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q61 – How should financial regulators deal with hybrid cases where tokens display investment-type features combined with other features (utility-type or payment- type characteristics)?

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

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

Q61.1 - Is there any other way financial regulators should deal with hybrid cases where tokens display investment-type features combined with other features?

Overall hybrid tokens should be considered as financial instruments with specific requirements. For instance, issuers should be required to publish information on the hybrid features of the token including: the specific rights attached to investors, the description of the project funded, etc. The EU disclosures framework can be inspired by that provided in France for ICOs.

FESE is of the opinion that any token that displays investment type features should be considered as a security; otherwise the utility or payment-type characteristic could potentially be used to cover a financial instrument, which could create a negative incentive for those issuers willing to escape from legal restrictions. Additionally, it should be taken into account that any investment feature has an impact on the nature of the asset that can displace the rest of the features (e.g. utility) with no legal implications. Thus, FESE considers advisable to separately apply the different regimes involved in the characteristics of the security and, consequently, this application of different regimes would include the application of securities regulation to any token that displays investment-type features. Furthermore, FESE sees merit in in establishing a dynamic in order to take into account that the investment-type features can change or not be displayed in the chronological evolution of the token. It should be clarified whether hybrid functions should not be permitted. Under the current framework, certain hybrid functions (e.g. payment) may be interpreted as incompatible with token classification as investment instruments. For example, MiFID II does not provide a definition of instruments of payment but specifies that they are excluded from the scope of 'transferable securities' (Article 4(1)(44)) and money-market instruments (Article 4(1)(17).

To prevent that digital hybrid assets act as "shadow"-digital securities and circumvent financial rules; the full regulation should be applicable. 'Investment/security tokens' should therefore be considered as financial instruments under MiFID II (Article 4, paragraph 15. Moreover, regulators should foresee a review-cycle of three years to reassess the developments of digital hybrid assets.

Q61.2 - Please explain your reasoning for your answer to question 61:

Where tokens display investment-type features combined with other features, hybrid tokens should be subject to regulations i.e. dealt with under securities law.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

1.2. Investment firms

Q62 - Do you agree that existing rules and requirements for investment firms can be applied in a DLT environment?

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

Q62.1 - Please explain your reasoning for your answer to question 62:

Rules for investment firms should apply and IT security elements should be aligned. The current regulation should reflect potential new financial services related to "digital assets". The focus should be put on the business model agreement rather than on the technical issues, as DLT used in a completely centralised business model should be compliant with current legislation. For decentralised platforms, there is merit in adapting regulation at application (smart contracts) and DLT level.

Q63 - Do you think that a clarification or a guidance on applicability of such rules and requirements would be appropriate for the market?

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

Q63.1 - Please explain your reasoning for your answer to question 63:

1.3. Investment services and activities

Q64 - Do you think that the current scope of investment services and activities under MiFID II is appropriate for security tokens?

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

Q64.1 - Please explain your reasoning for your answer to question 64:

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q65 - Do you consider that the transposition of MiFID II into national laws or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT for investment services and activities? Please explain your reasoning.

At this stage, it seems difficult to assess the impact of the transposition of MIFID II regarding the use of DLT as it is a vast regulation with a wide range of legal implications. However, it should be noted that the use of DLT mainly depends on the specific adaptation of those particular legal concepts that could have an impact on the effective deployment of DLT technology, rather than a significant shift of the current core legislation. FESE would imagine that one of the main difficulties consists in the succession of several transposition processes in a relatively short period of time that could entail relevant costs of adaptation for the industry.

1.4. Trading venues

Q66 - Would you see any particular issues (legal, operational) in applying trading venue definitions and requirements related to the operation and authorisation of such venues to a DLT environment which should be addressed? Please explain your reasoning.

A company offering a "crypto-asset"-trading platform should be subject to the same transparency regime as "traditional" trading venues. Considering 'investment/security tokens' as financial instruments implies that the existing regulatory frameworks also apply to "crypto-asset"-trading platforms, allowing for a safe and transparent trading environment for both investors and issuers. FESE believes that the existing MiFID framework for trading venues can be applied to "crypto-asset"-trading platforms and that there is no reason to adopt special provisions for "crypto-asset" offerings. FESE would propose that "digital-assets" should be traded on trading venues as defined in MiFID II/MiFIR only (i.e. on regulated markets, MTFs or OTFs). Trading venues should be responsible for providing and ensuring equal market rules, market integrity, detecting and sanctioning mistraces. However, regulatory requirements should be balanced in order to account for the nature of the potential investors and issuers. In addition, further detail will be needed to specify technology risks that any potential investor would face (e.g. a loss of the cryptographic keys, unexpected failures of the DLT network due to unknow or unexpected errors in Blockchain technology or changes in the underlying blockchain technology) in the information documents. In terms of suitability assessment, the current legal framework ensures that the suitability of any investment is checked for every investor and, therefore, it is unlikely that deep changes would be needed. However, it should be noted that blockchain knowledge is essential and it should thus be advisable to include such knowledge in the curricular certifications of investment advisors to ensure a proper suitability assessment.

1.5. Investor protection

Q67 - Do you think that current scope of investor protection rules (such as information documents and the suitability assessment) are appropriate for security tokens?

Please explain your reasoning.

Yes, security tokens meets the definition of a specified investment and therefore fall within the regulatory perimeter of the supervisory authorities. Investor protection rules are appropriate for "digital-assets". Potential amendments of such rules, as a result of the MiFID Review, should consider specific risks attached to "digital-assets". To realise the potential of the new asset class, the usual rules should apply and, if necessary, additional IT related requirements shall also apply (e.g. safeguarding the integrity of a DLT-network).

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q68 - Would you see any merit in establishing specific requirements on the marketing of security tokens via social media or online?

Please explain your reasoning.

N/A

Q69 - Would you see any particular issue (legal, operational,) in applying MiFID investor protection requirements to security tokens?

Please explain your reasoning.

N/A

1.6. SME Growth Markets

Q70 - Do you think that trading on DLT networks could offer cost efficiencies or other benefits for SME Growth Markets that do not require low latency and high throughput?

Please explain your reasoning.

In technical terms, DLT could be appropriate for SME Growth Markets and other segments that do not require low latency and high throughput or scalability. Real time settlement can impact on liquidity and capital requirements of larger and deeper markets and in this sense, the creation of a "sandbox" environment could provide a platform to gain experience on the applicability of DLT and DLT systems governance for listed SMEs in EU capital markets. However, it should be noted that DLT systems are currently not only slower than existing legacy systems but there are also problems of price transparency/arbitrage and DLT cannot be used to centralise orders due to the inherent nature of the technology, and therefore does not allow for producing an efficient price formation mechanism.

1.7. Systems resilience, circuit breakers and electronic trading

Q71 - Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed?

Please explain your reasoning (if needed).

FESE does not see particular issues as long as security tokens fall under existing financial market regulation. Resilience measures are important, and regulators should always ensure clear responsibilities.

1.8. Admission of financial instruments to trading

Q72 – Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed?

Please explain your reasoning.

FESE does not see particular issues as long as security tokens fall under existing financial market regulation. In addition, trading venues have developed appropriate rules and principles in accordance with their high standards and regulatory requirements. For "crypto-asset"-trading platforms, it is important for the purposes of market and consumer protection to enforce rules, bringing them to the standards adhered to by established financial market infrastructures. Admission to trading should only be allowed by trading venues (i.e. regulated markets, MTFs or OTFs), and should follow the same rules as today. The admission for third-country participants should also follow the current MiFID II regime (until there is a MiFID II

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

equivalence decision taken, national regimes apply for third-country firm access to European trading venues). However, allowing "crypto-assets" to trading may shift the responsibility from an issuer to the operator (as no issuer exists), also with regard to the monitoring of technical issues (like forks). In addition, the physical settlement would require relevant regulated settlement systems being in place.

1.9. Access to a trading venues

Q73 - What are the risks and benefits of allowing direct access to trading venues to a broader base of clients?

Please explain your reasoning.

Today, only financial intermediaries are allowed to have access to trading venues. The expansion to a broader base of clients not subject to prudential supervision contradicts the current understanding of a Financial Market Infrastructure. The current restriction to supervised participants is intended to ensure compliance with and enforcement of financial market regulations.

1.10. Pre and post-transparency requirements

Q74 - Do you think these pre- and post-transparency requirements are appropriate for security tokens?

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

Q74.1 - Please explain your reasoning for your answer to question 74:

Security tokens should be treated as normal transferable securities and therefore existing financial market regulations should comply with corresponding transparency rules. Lower transparency standards are therefore not justifiable. Pre- and post-trade transparency obligations have to apply; to allow investors to have access to the market data (opportunities, information) and to have a clear idea of the liquidity of the product before investing. Transparency is also necessary for the best execution assessment. It is vital that the MiFIR requirements on transparency for trading venues (both for equity and non-equity instruments) apply in the same way for "crypto-assets" as they currently apply for any other financial instrument. Therefore, 'security tokens' need to be able to report the number of details identifying the financial instrument that are required for a reporting through an Approved Publication Arrangement (APA), e.g. the identifier of the financial instrument; the price, volume and the time of the transaction or the code for the trading venue. This information ensures the integrity of markets, by enabling national competent authorities (NCAs) and ESMA to enforce this integrity by monitoring investment firms' activities as to their honest, fair and professional market behaviour. In order to detect and investigate potential market abuse, any transactions of a reportable financial instrument, including "digital- assets", need to be covered by the transaction reporting requirements to safeguard the integrity of the financial market. FESE believes that pre- and post-transparency provided via an APA and ARM plays a key role for the stability of the financial market. Trades and transactions in 'security tokens' should be reported via an APA in order to maintain the achievements in regard to financial stability so far.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q75 - Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed (e.g. in terms of availability of data or computation of thresholds)? Please explain your reasoning.

FESE does not see particular issues as long as 'security tokens' fall under existing financial market regulation. The thresholds should be adapted to this product type. Transparency is necessary for the information of the investors and the liquidity of the market.

1.11. Transaction reporting and obligations to maintain records

Q76 - Would you see any particular issue (legal, operational) in applying these requirements to security tokens which should be addressed?

Please explain your reasoning.

FESE does not see particular issues as long as security tokens fall under existing financial market regulation.

Market Abuse Regulation (MAR)

2.1. Insider dealing

Q77 - Do you think that the current scope of Article 8 of MAR on insider dealing is appropriate to cover all cases of insider dealing for security tokens?

Please explain your reasoning

The same rules should apply, however a special focus/adaption to the specifics of the IT environment and the creation of crypto-assets might be necessary to prevent price-manipulation (e.g. creation of unknown volumes of some "crypto-assets"). Supervisory bodies may have to adapt. Adaptations may be necessary to cover all cases of insider dealing, as: 1) The language and wording used covers traditional financial instruments/trading venues. Technical language appropriate to security tokens should be included 2) It must also be reviewed if new types of involved persons related to the issuer, the "sponsors" and the IT providers should be defined and included in article 8.4. In addition, new type of frauds may create new type of sensitive information. Please note that should 'investment/security tokens' not be classified as financial instruments, and not be in the scope of MAR, it will be necessary to re-write the global text to make a clear separation between requirements linked with financial instruments and those linked with 'investment/security tokens'.

2.2. Market manipulation

Q78 - Do you think that the notion of market manipulation as defined in Article 12 of MAR is sufficiently wide to cover instances of market manipulation of security tokens?

Please explain your reasoning

Market manipulation is generally closely linked with the way trading venues' rules are designed and the way rules are embedded in the trading engine. FESE believes that the way the blockchain trading platform will be designed will certainly have an impact on the market manipulation scenarios. MAR Annex 1 will have to be reviewed to include provisions for trading platforms using DLT technology.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q79 - Do you think that there is a particular risk that manipulative trading in crypto- assets which are not in the scope of MAR could affect the price or value of financial instruments covered by MAR?

FESE considers that this risk exists if the relevant "crypto-assets" have a correlation in their value with any financial instruments covered by MAR, via their smart contracts or their underlying features. Thus, it could be foreseeable that extensive changes in the demand of said "crypto-assets" could potentially have cross implications with the financial instruments to which they are correlated. This should be carefully analysed.

We foresee potential operational risks derived from validator nodes implicit within the DLT environment that could result in market manipulation (agreement between several nodes to incorporate false transactions into the chain, adding of the same transaction several times onto the chain, delay in the inclusion of transactions to the chain or remaining of a valid transaction outside the chain amongst others).

In this regard, FESE suggests intense monitoring in order to identify responsibilities and proper functioning of the managers of platforms and allow for flagging the actions considered as manipulations of market.

FESE supports the OECD opinion that "crypto-assets" can be used as a leading price indicator for an underlaying market, in a similar way as derivatives are used as leading price indicators for the asset in which they are based.

Fraudulent or manipulative trading in "crypto-assets" linked with financial instruments could also be a risk from listed companies operating "crypto-assets"-trading platforms. The latter could affect the value or the price of financial instruments.

Short Selling Regulation (SSR)

Q80 - Have you detected any issues that would prevent effectively applying SSR to security tokens? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

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

Q80.1 - Is there any other issue that would prevent effectively applying SSR to security tokens?

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

Q80.2 - Please explain your reasoning for your answer to question 80:

The SSR applies to the global position held by the holder. In this sense, concluding that a sale operation violates the SSR is currently difficult, since the rest of the holder's position is not known beforehand (he/she might be selling shares while buying futures).

Q81 - Have you ever detected any unregulated crypto-assets that could confer a financial advantage in the event of a decrease in the price or value of a share or sovereign debt?

Please explain your reasoning:

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Prospectus Regulation (PR)

2.3. Scope and exemptions

Q82 - Do you consider that different or additional exemptions should apply to security tokens other than the ones laid down in Article 1(4) and Article 1(5) of PR?

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

Q82.1 - Please explain your reasoning (if needed).

FESE supports nascent technologies that provide new means of sourcing finance for companies in a safe and regulated way. However, ESMA has in the context of "crypto-assets" and ICOs, raised concerns regarding investor protection (specifically whether investors are aware of the level of risk involved) and firms conducting business without applying EU legislation. In an own initiative report, the ESMA Securities and Markets Stakeholders Group (SMSG) underlines the importance of legal certainty in ICOs and "crypto-assets". The report points to the need for clarification regarding the application of existing financial regulation to virtual assets. Such clarification is necessary given the very divergent national regulatory approaches to "crypto-assets". FESE also welcomes that the Commission is considering potential regulatory measures to address "crypto-assets", currently not covered by EU legislation.

FESE considers that it is important to establish key principles upon which the EU can build a role in facilitating the development and implementation of FinTech. These principles include the need for:

• The application of the same rules for the same services and risks (including across different pieces of legislation) based on the principle of technology neutrality.

• A risk-based approach built on proportionality and materiality which allows for flexibility, particularly in respect of innovation with small groups of customers (i.e. sandboxes), while ensuring a level playing field across the EU.

• A balancing of the local (country) risks alongside the benefits of cross-border markets (i.e. scalability, interoperability and passporting of services).

ICOs may play a role for company financing at an early stage but should not be seen as an alternative to IPOs. If exemptions or different rules were to be applied, this could risk creating issues in terms of investor protection as well as level playing field for exchanges that apply a full range of EU trading rules to ensure market integrity, price formation, and consumer protection.

Additionally, it might be useful to inform in the prospectus about the technological features of the "crypto-assets", especially if a smart contract is included. Furthermore, if smart contracts are being utilised, there should be a requirement to obtain a certificate from an auditing firm that the programmed algorithm functions exactly as laid out in the prospectus. Ideally, this information should be summarised in an understandable manner to reduce the complexity and the length of the prospectus and costs.

As security tokens are securities, they must be able to be identified via an ISIN. This would also help to process security tokens in established IT systems. To our knowledge, some numbering agents have confirmed that they have started to allocate ISINs to tokens (mostly securities tokens). Beyond ISIN (relevant for security tokens, and possibly hybrid

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

tokens), some other existing global identifiers could also be used, for instance the ISO 4217 currency code could very well be used for "crypto-assets", providing similar benefits to the market than the one referred to so far for securities. We generally promote the adoption of established ISO standards for the identification of "digital-assets", while recognising that we will likely need a separate, additional other "digital-asset"-identifier, at least for those assets that are neither securities nor currencies.

As the technology is new, investors would need more information on: (where applicable) which type of chain is used (public vs private / permissioned vs permissionless)? Which type of smart contract is used? Which type of safety and resilience measures are applied in the used smart contracts (e.g. technical malfunction detection tools)? Which type of token governance mechanism is included? Which types of risks are addressed e.g. technological, economical or environmental? It could be beneficial to aggregate this information into a rating for investors about the asset in question, provided by a trusted third party.

2.4. The drawing up of the prospectus

Q83 - Do you agree that Delegated Regulation (EU) 2019/980 should include specific schedules about security tokens?

☒Yes
☐No
☐Don't know / no opinion/not relevant

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

Prospectus schedules for security token offerings should take into account the technology accompanying these products as it constitutes an important part of the listing operation. This means certain points related to this technology should be included in the prospectus for the benefit of investors, in particular:

- type of blockchain used (private/public/permissioned);
- type of safety and resilience measures applied to smart contracts (the description of cybersecurity devices and which technical malfunction detection tools are used);
- typology of smart contracts;
- token governance mechanisms or, otherwise, the divisibility of tokens;
- costs associated with the use of the underlying blockchain;
- different guarantees in relation to the underlying technology (financial guarantees, private key regeneration, etc.);
- detailed description of the risks incurred by the investor, whether they are economic, technological or related to the project itself;
- type of customers, as well as the jurisdictions, that have access to the subscription (coded information on the smart contracts);

Nature and classification of the investment token should be readily identifiable by investors (and regulators).

The summary should contain a brief description of:

- Underlying value and nature of investor rights/ claim (membership/ voting and financial participation rights, claim against legal counterparty – right to receive funds, underlying base value)
- Existence of underlying assets

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

- Hybrid features of the token/ target use beyond investment (e.g. unit of exchange, utility). In case of utility tokens, a description of the ecosystem the token is attached to, development stage, milestones and utilisation rights of the tokenholder)
- Offer:
  - Structure of the offering – including stages, price and volume at each
  - Trading/ transfer - secondary market liquidity (availability on regulated market, MTF or 'unregulated'/ out-of-scope "crypto-asset"-trading platforms)

Q84 - Do you identify any issues in obtaining an ISIN for the purpose of issuing a security token?

FESE has not yet identified any issues in obtaining an ISIN for security tokens.

Q85 - Have you identified any difficulties in applying special types of prospectuses or related documents (i.e. simplified prospectus for secondary issuances, the EU Growth prospectus, the base prospectus for non-equity securities, the universal registration document) to security tokens that would require amending these types of prospectuses or related documents?

Please explain your reasoning.

Article 18 of the Prospectus Regulation provides a degree of flexibility in scenarios where information required by Delegated Regulation (EU) 2019/980, is not adapted to 'investment/security tokens' or the activities of the token issuers. Level 2 measures may be appropriate to specify the scenarios where this article could be availed of.

Q86 - Do you believe that an *ad hoc* alleviated prospectus type or regime (taking as example the approach used for the EU Growth prospectus or for the simplified regime for secondary issuances) should be introduced for security tokens?

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

Please explain your reasoning for your answer to question 86:

Q87 - Do you agree that issuers of security tokens should disclose specific risk factors relating to the use of DLT?

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q87.1 - Please explain your reasoning for your answer to question 87

Security tokens should be subject to the Prospectus Regulation and their offer to the public should be subject to the drafting of a prospectus. To that end, we would support amendments to the Prospectus Regulation to include prospectus schedules catering to the specifics of the issuance of security tokens. This would mirror the approach taken to different asset classes in the current framework – same high-level rules with tailored implementation depending on the security. Any specific risk related to the use of DLT should be addressed via the operator of the platform. FESE considers there is merit in evaluating the requirements on information about decentralised governance, including the terms and conditions of the participants describing the different roles when appropriate. As ESMA's guidelines on risks factors make a generic description of risks in a way that can be suitable for any kind of risks, including the technological ones, FESE considers these guidelines are mostly adequate for a scenario in which "crypto-assets" are under their scope. Nevertheless, it would be advisable to add in the Appendix I of the Guidelines some examples of technologic risk associated with blockchain (e.g. a lost in the cryptographic keys, unexpected failures of the DLT network due to unknow or unexpected errors in blockchain technology or changes in the underlying blockchain technology).

Central Securities Depositories Regulation (CSDR)

Q88 - Would you see any particular issue (legal, operational, technical) with applying the following definitions in a DLT environment?

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

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

Q88.1 - Is there any other particular issue with applying the following definitions in a DLT environment?

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

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

Looking at the purpose of CSDR, it can be concluded that the regulation is drafted in a technology-neutral way as to regulate all types of financial instruments falling under its scope. Our legal analysis allows us to consider that central depositories are authorised to manage security tokens as "securities" within its regulatory framework. Central depositories can therefore continue to play an important role in ensuring that appropriate risk measures are taken to service this type of asset.

In FESE's view, definitions should be adapted when there is a real decentralised governance and therefore a decentralised business model. For systems managed by a central entity using DLT some definitions like "security accounts" could need some minor updates.

FESE´s view is that CSDR is technologically neutral.

However, this regulation is drafted based on centralised ledgers and FESE would therefore support review to ensure neutrality as to the underlying technology whilst safeguarding the financial markets.

In FESE's view, the current know-how and level of protection of regulated market infrastructures can only be contributing to the development of a safe environment for "crypto-assets". Thus, the provision of CSD services should always be subject to regulation and compliance with certain conditions regardless of the technology used for the provision of the service and the evolution into this new environment should be ensured for the existing market infrastructures.

Q88.2 - Please explain your reasoning for your answer to question 88:

Any service provider offering CSD-like services (core services pursuant to Section A of the annex to CSDR, i.e. notary service, central maintenance and settlement services) should comply with the CSDR and SFD, independent of the used technology. These functions are important for market integrity.

To allow institutional investors to participate from the technological benefits of "digital-assets", those assets need to fulfil the necessary required governance standards (which are e.g. a record of the existence of a security and a conformation about the total amount securities issued). This also ensures investor protection.

CSDs should be allowed to hold "crypto-assets" and other "digital assets", even if these neither qualify as a security nor have a payment function. Hence, a new category needs to be introduced in the CSDR/SFD.

Q89 - Do you consider that the book-entry requirements under CSDR are compatible with security tokens?

☒Yes

☐No

☐Don't know / no opinion/not relevant

Q89.1 - Please explain your reasoning for your answer to question 89:

CSDR do not prescribe any technical execution method for the registration of securities and at the same time, the notion of a 'securities account' is defined in CSDR in a broad way, i.e. "an account on which securities can be credited or debited". It is our view this definition could encompass recording on a permissioned DLT account. If questions about legal certainty and compatibility arise at national level as the recognition of ownership and other entitlement in securities transferred through registration in account is governed

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

by domestic legislation, the national legislator could consider clarifying it (e.g. in France, recording on DLT was clarified as having equivalent effects to the book-entry on an account).

Q90 - Do you consider that national law (e.g. requirement for the transfer of ownership) or existing market practice in your jurisdiction would facilitate or otherwise prevent the use of DLT solution?

Please explain your reasoning.

N/A

Q91 - Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment?

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

	1	2	3	4	5	No opinion
Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system	X					
Rules on measures to prevent settlement fails	X					
Organisational requirements for CSDs	X					
Rules on outsourcing of services or activities to a third party		X				
Rules on communication procedures with market participants and other market infrastructures	X					
Rules on the protection of securities of participants and those of their clients		X				
Rules regarding the integrity of the issue and appropriate reconciliation measures		X				
Rules on cash settlement		X				
Rules on requirements for participation	X					
Rules on requirements for CSD links		X				
Rules on access between CSDs and access between a CSD and another market infrastructure			X			

Q91.1 - Is there any other particular issue with applying the current rules in a DLT environment, (including other provisions of CSDR, national rules applying the EU acquis, supervisory practices, interpretation, applications...)?

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

No, although these requirements need to be clarified in the way they could be met. In particular, as regards rules on cash settlement, we believe that the following requirements are not barriers to the use of DLT: **Recording on an account in a book-entry form and definition of securities accounts.** CSDR does not prescribe any technical execution method for the registration of securities. At the same time, the notion of a 'securities account' is defined in CSDR in a broad way, i.e. "an account on which securities can be credited or debited". It is our view that this definition could encompass recording on a permissioned DLT account. The only possible questions may arise at national level as the recognition of ownership and other entitlement in securities transferred through registration in account is governed by

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

domestic legislation. This clarification has already been made in some countries, e.g. in France, recording on DLT was clarified as having equivalent effects to the book-entry on an account.
Requirement to settle transactions on a Delivery-versus-Payment (DvP) basis (Article 39.7). The fundamental need for DvP is to remove the settlement risk between market participants. Hence, whenever the transaction is against cash, but not using a DvP mechanism, it would leave market participants exposed to possible substantial risk. Therefore, any technology used for transferring securities of other investments should offer an interface or link to the relevant payment solution to maintain the same level of risk mitigation.
Obligation of settlement in CoBM or CeBM (Article 40), which contains requirements on the use of Central Bank Money or, where it is not practical and available, complying with the CSDR ancillary banking services section, containing the limits on the use of Commercial Bank Money without a banking licence or usage of a limited purpose bank (examples which do not exist yet). However, the Article is not technology-specific and cost-related considerations arise in the same manner for all operators. In our view, the requirements of the ancillary banking section may need to be adjusted to adequately respond to average market CoBM CSD needs.

For the following points, although we do not see them as barriers, regulatory guidance on how CSDs could comply with the provisions in the DLT context would be appreciated:

- Exercising trading, settlement and custody in a single legal entity, provided that the risks are catered and relevant for the activity legislation is complied with requirements related to segregation of accounts and reconciliation may be achieved in a different way.
- Accounting certainty, auditability and data protection (requirements related to segregation of accounts and reconciliation) may be achieved in a different.

Q91.2 - Please explain your reasoning for your answer to question 91:

FESE considers that if 'investment/security tokens' have the same characteristics as MiFID II's financial instruments, these tokens should be required to apply the relevant existing regulation as clarified in the ESMA Advice on Initial Coin Offerings and Crypto-Assets .

We believe that CSDR is not a barrier to the implementation of DLT, as it does not prevent its use.

Q92 - In your Member State, does your national law set out additional requirements to be taken into consideration, e.g. regarding the transfer of ownership (such as the requirements regarding the recording on an account with a custody account keeper outside a DLT environment)?

Please explain your reasoning.

N/A

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Settlement Finality Directive (SFD)

Q93 - Would you see any particular issue (legal, operational, technical) with applying the following definitions in the SFD or its transpositions into national law in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

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

Q93.1 - Is there any other particular issue with applying the following definitions in the SFD or its transpositions into national law in a DLT environment?

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

In FESE view, definitions should be adapted when there is a real decentralised governance and therefore a decentralised business model. For systems managed by a central entity using DLT some definitions like “security accounts” could need some minor updates.

SFD definitions should not be changed or reviewed because of new technologies. This is a principle applicable to any current regulation, directive or national law. However, upcoming regulations must consider and take into account technological evolution.

It would be beneficial to have clarity by policy-makers on how some concepts apply in the DLT context.

- To foster finality of relevant instructions, the definition of SSS or PSS would need to cover all relevant token and crypto “asset” service providers. Consequently, all providers would need to comply with SFD (and other applicable regulation, such as CSDR).
- A system operator must be responsible for the relevant SSS/PSS. Consequently, only private blockchain solutions are viable.
- Therefore, the regulators should ensure that requirements of CSDR and SFD are not circumvented by DLT.

Q93.2 - Please explain your reasoning for your answer to question 93.

N/A

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q94 - SFD sets out rules on conflicts of laws. According to you, would there be a need for clarification when applying these rules in a DLT network (in particular with regard to the question according to which criteria the location of the register or account should be determined and thus which Member State would be considered the Member State in which the register or account, where the relevant entries are made, is maintained)?

Please explain your reasoning.

Yes, we would appreciate such clarity. The location of an asset constituted on a DLT and the possible span of a DLT over several jurisdiction, could prevent the use of current conflict of laws solutions.

Q95 - In your Member State, what requirements does your national law establish for those cases which are outside the scope of the SFD rules on conflicts of laws?

N/A

Q96 - Do you consider that the effective functioning and/or use of DLT solution is limited or constrained by any of the SFD provisions?

☐Yes
☒No
☐Don't know / no opinion/not relevant

Q96.1 - If you do agree that the effective functioning and/or use of DLT solution is limited or constrained by any of the SFD provisions, please provide specific examples (e.g. provisions national legislation transposing or implementing SFD, supervisory practices, interpretation, application,...). Please explain your reasoning.

N/A

Q96.1 - Please explain your reasoning for your answer to question 96:

We perceive that this is not the case. CSDs have sufficient clarity and believe that SFD provides sufficient certainty.

Financial Collateral Directive (FCD)

Q97 - Would you see any particular issue (legal, operational, technical) with applying the following definitions in the FCD or its transpositions into national law in a DLT environment?

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

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q97.1 - Is there any other particular issue with applying the following definitions in the FCD or its transpositions into national law in a DLT environment?

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

As referenced above, in order to achieve the necessary and desirable legal certainty, FESE considers it beneficial to have clarity by policy-makers on how the FCD concept apply in the DLT context.

Q97.2 - Please explain your reasoning for your answer to question 97:

N/A

Q98 - FCD sets out rules on conflict of laws. Would you see any particular issue with applying these rules in a DLT network?

We consider that additional clarity would be desirable.

Q99 - In your Member State, what requirements does your national law establish for those cases which are outside the scope of the FCD rules on conflicts of laws?

N/A

Q100 - Do you consider that the effective functioning and/or use of a DLT solution is limited or constrained by any of the FCD provisions?

☐Yes
☒No
☐Don't know / no opinion/not relevant

Q100.1 - If you do agree that the effective functioning and/or use of a DLT solution is limited or constrained by any of the FCD provisions, please provide specific examples (e.g. provisions national legislation transposing or implementing FCD, supervisory practices, interpretation, application, ...).

Please explain your reasoning.

Q100.1 - Please explain your reasoning for your answer to question 100:

European Markets Infrastructure Regulation (EMIR)

Q101 - Do you think that security tokens are suitable for central clearing?

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q101.1 - Please explain your reasoning (if needed).

Risk Management services of CCPs will still be required in the future, as the financial crisis 2008 has brought to light. The G20 declaration of Pittsburgh strengthened the importance of CCPs in this context. Other important functions of CCPs including multilateral netting and netting between different asset-classes, collateral and default management processes cannot be directly replaced by DLT today. We believe that digital securities are appropriate for central clearing, therefore CCPs should be allowed to clear them in accordance with EMIR. Further clarity is needed under which conditions / prudential requirements CCPs are allowed to clear other digital-assets / derivatives with a "digital asset" underlying. They should also qualify as eligible margins In general, we believe that the relevant regulations are agnostic to the kind of systems that may be used by a CCP/TR. However, it would need to be clarified that a CCP may accept and hold digital security and payment assets for settlement and margining purposes. The possibility of "T-instant" is no unique feature to DLT. However, as of now there seems to be a majority of participants in the market preferring T+2 due to e.g. liquidity management reasons. Risks with regard to insolvency and (physical) delivery are also still relevant. Using DLT would allow to segregate accounts and margin custody. This should be allowed by regulation.

Q102 - Would you see any particular issue (legal, operational, technical) with applying the current rules in a DLT environment? Please rate each proposal from 1 to 5, 1 standing for "not a concern" and 5 for "strong concern".

	1	2	3	4	5	No opinion
Rules on margin requirements, collateral requirements and requirements regarding the CCP's investment policy	X					
Rules on settlement			X			
Organisational requirements for CCPs and for TRs	X					
Rules on segregation and portability of clearing members' and clients' assets and positions	X					
Rules on requirements for participation	X					
Reporting requirements				X		

Q102.1 - Is there any other particular issue (including other provisions of EMIR, national rules applying the EU acquis, supervisory practices, interpretation, applications, ...) with applying the current rules in a DLT environment?

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

N/A

Q102.2 - Please explain your reasoning for your answer to question 102:

FESE believes that central clearing can be DLT processed, but at the same time it should be centrally governed, and the transfer of ownership and finality would need to be clearly provided for by applicable law: in this case, the relationship between the participant is not altered. The DLT technology should not per se fundamentally change the existing legal framework, and therefore, the use of cryptography and DLT as the only differentiator factor for "crypto-assets" may be considered insufficient. Also, settlement finality rules

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

should be in line with the system finality using a DLT. Using DLT, segregated accounts and margin custodized should be enabled by relevant regulation.

In addition, FESE is of the opinion that several topics should be clarified under EMIR, for instance:

- Could CCPs clear "crypto assets" such as tokens representing non-regulated assets? Under what conditions? If these tokens are not defined as financial contracts, would they be subject to EMIR?
- Would derivatives whose underlying is a "crypto-asset" be subject to EMIR? Would there be additional prudential requirements for such types of assets?
- Will market infrastructures in general, and CCPs in particular, be allowed to provide services related to access to a DLT in order to facilitate participation of all market participants?

Q103 - Would you see the need to clarify that DLT solutions including permissioned blockchain can be used within CCPs or TRs?

N/A

Q104 - Would you see any particular issue with applying the current rules to derivatives the underlying of which are crypto assets, in particular considering their suitability for central clearing?

Please explain your reasoning (if needed).

N/A

The Alternative Investment Fund Directive

Q105 - Do the provisions of the EU AIFMD legal framework in the following areas are appropriately suited for the effective functioning of DLT solutions and the use of security tokens?

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

	1	2	3	4	5	No opinion
AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;						
AIFMD provisions requiring AIFMs to maintain and operate effective organisational and administrative arrangements, including with respect to identifying, managing and monitoring the conflicts of interest;						
Employing liquidity management systems to monitor the liquidity risk of the AIF, conducting stress tests, under normal and exceptional liquidity conditions, and ensuring that the liquidity profile and the redemption policy are consistent;						
AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets;						

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments.						

Q105.1 - Is there any other area in which the provisions of the EU AIFMD legal framework are appropriately suited for the effective functioning of DLT solutions and the use of security tokens?

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

N/A

Q105.2 - Please explain your reasoning for your answer to question 105:

N/A

Q106 - Do you consider that the effective functioning of DLT solutions and/or use of security tokens is limited or constrained by any of the AIFMD provisions?

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

Q106.1 - If you do consider that the effective functioning of DLT solutions and/or use of security tokens is limited or constrained by any of the AIFMD provisions, please provide specific examples with relevant provisions in the E U a c q u i s .

Please explain your reasoning (if needed).

N/A

Q106.2 - Please explain your reasoning for your answer to question 106:

N/A

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

Q107 - Do the provisions of the EU UCITS Directive legal framework in the following areas are appropriately suited for the effective functioning of DLT solutions and the use of security tokens?

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

	1	2	3	4	5	No opinion
Provisions of the UCITS Directive pertaining to the eligibility of assets, including cases where such provisions are applied in conjunction with the notion "financial instrument" and/or "transferable security"						
Rules set out in the UCITS Directive pertaining to the valuation of assets and the rules for calculating the sale or issue price and the repurchase or redemption price of the units of a UCITS, including where such rules are laid down in the applicable national law, in the fund rules or in the instruments of incorporation of the investment company;						

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

UCITS Directive rules on the arrangements for the identification, management and monitoring of the conflicts of interest, including between the management company and its clients, between two of its clients, between one of its clients and a UCITS, or between two - UCITS;						
UCITS Directive provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens;						
Disclosure and reporting requirements set out in the						
UCITS Directive.						

Q107.1 - Is there any other area in which the provisions of the EU UCITS Directive legal framework are appropriately suited for the effective functioning of DLT solutions and the use of security tokens?

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

N/A

Q107.2 - Please explain your reasoning for your answer to question 107:

N/A

Other final comments and questions as regards security tokens

Q108 - Do you think that the EU legislation should provide for more regulatory flexibility for stakeholders to develop trading and post-trading solutions using for example permissionless blockchain and decentralised platforms?

☐Yes
☒No
☐Don't know / no opinion/not relevant

Q108.1 - If you do think that the EU legislation should provide for more regulatory flexibility for stakeholders to develop trading and post-trading solutions using for example permissionless blockchain and decentralised platforms, please explain the regulatory approach that you favour.

Please explain your reasoning.

N/A

Q108.2 - Please explain your reasoning for your answer to question 108:

Europe should create an environment which fosters innovation, while preserving financial stability and market integrity. A common legal framework is beneficial in creating legal certainty for new products. The application of existing regulations is an important component for that certainty.

FESE does not support the development of trading or post-trading activities on permissionless and decentralised governed platforms for the following reasons:

- It is not possible to hold anyone accountable in case of fraud or illegal activities.
- Compliance with regulation will not be enforceable. Applicability of any regional regulation will be contested.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

- For the reasons raised above, there will be no way to ensure services abide by basic global obligations in terms of AML/CFT, consumer protection or market abuse.
- Activity will remain opaque to market authorities as there is no accountable entity responsible for providing transparency.
- Competitive issues will arise with existing providers who need to bear high fixed costs in order to comply with existing requirements.
- Liquidity risk will be higher due to a transfer of the activity to unregulated open networks out of reach of current market authorities.
- As a result of an unregulated but connected activity, there is a risk of contagion to traditional markets in case of a credit crisis in the DLT systems.

Q109 - Which benefits and risks do you see in enabling trading or post-trading processes to develop on permissionless blockchains and decentralised platforms?

"Decentralised" solutions risk operating with an absence of proper accountability and raise practical question of how existing regulatory frameworks (MAR, MiFID II, Transparency Directive, Anti-Money Laundering Directive, GDPR) can be effectively applied in the absence of an identifiable "operator", "controller" or centralised governance scheme. In some cases, there may still be entities (developers or controllers) with enough residual control/ influence to apply accountability. Other models may be less clear. In either case, it would be logical to address risks (consumer protection, financial stability, and money laundering and terrorist financing risk categories) by regulating the functions of identifiable participants that interact with the venue.

FESE does not support the development of trading or post-trading activities on permissionless and decentralised governed platforms for the following reasons:

- It is not possible to hold anyone accountable in case of fraud or illegal activities.
- Compliance with regulation will not be enforceable. Applicability of any regional regulation will be contested.
- For the reasons raised above, there will be no way to ensure services abide by basic global obligations in terms of AML/CFT, consumer protection or market abuse.
- Activity will remain opaque to market authorities as there is no accountable entity responsible for providing transparency.
- Competitive issues will arise with existing providers who need to bear high fixed costs in order to comply with existing requirements.
- Liquidity risk will be higher due to a transfer of the activity to unregulated open networks out of reach of current market authorities.

As a result of an unregulated but connected activity, there is a risk of contagion to traditional markets in case of a credit crisis in the DLT systems.

Q110 - Do you think that the regulatory separation of trading and post-trading activities might prevent the development of alternative business models based on DLT that could more efficiently manage the trade life cycle?

☒Yes
☐No
☐Don't know / no opinion/not relevant

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q110.1 - If you do think that the regulatory separation of trading and post-trading activities might prevent the development of alternative business models based on DLT that could more efficiently manage the trade life cycle, please identify the issues that should be addressed at EU level and the approach to address them.

Please explain your reasoning.

FESE agrees that the current regulatory separation of trading, clearing and settlement prevents alternative business models. However, we are cautious as to whether alternative models would be more efficient.

These models based on atomic instant settlement may provide a more efficient solution to some of the current business processes. FESE believes that primary markets are specially fit to be managed in DLT in an integrated manner. The risks would be highly reduced by providing instant placing and settlement of primary issuances.

However, integrated atomic settlement cannot be more efficient when servicing secondary markets for the following reasons:

- There is a need for the T+2 settlement cycle in cash equities and bonds markets. For instance, market liquidity providers often take positions in the market that they distribute later among different clients, who need to be identified across the settlement chain. It must be also considered that international investors need to deal with markets in different time zones.
- Separation of functions allows for netting. Netting can take place at clearing level by a CCP, but technical netting also takes place at settlement level. Netting efficiency means that only a small portion of the cash and the assets are actually required to close the positions that have been traded.

Treasurers need time to manage their treasury pools and anticipate their liquidity requirements. Having to settle all transactions atomically and in real time would create liquidity frictions across market and institutions and increase the cost of financing.

The split of infrastructures could be a small brake for this market, since the ability to integrate all activities is one of the essential characteristics of DLT environments. However, it is a necessary separation for the delimitation of responsibilities and their framing within the current regulation.

The effort made by the entire industry promoted by the EMIR legislation was made because it was considered essential that CCPs cannot carry out any other activity, since they have a key role for European financial market stability. Going back on this concept would be counterproductive.

On the other hand, the fact that the trading is carried out at a different time from the register of operations is not due to a technological impediment, but to a business need. If all the trades that are carried out in a market must be cleared sequentially, the impossibility to clear one of them produces a chain effect that prevents many others that occur afterwards from being cleared. To avoid these effects, it is necessary to be able to isolate the non-cleared transaction and allow the clearing of the rest. This is a process that cannot be carried out in real time.

Q110.2 - Please explain your reasoning for your answer to question 110:

N/A

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q111 - Have you detected any issues beyond those raised in previous questions on specific provisions that would prevent effectively applying EU regulations to security tokens and transacting in a DLT environment, in particular as regards the objective of investor protection, financial stability and market integrity?

☒Yes

☐No

☐Don't know / no opinion/not relevant

Q111.1 - Please provide specific examples and explain your reasoning for your answer to question 111:

Yes, especially in what is related to investor´s rights. In the first place, FESE considers crucial that this prospective legislation includes a specific rule for conflicts of law in order to provide certainty as to which law is applicable to the "crypto-asset" in question.

The challenge with "crypto-assets" is that, as DLT implies multiple locations, there may not be a single connection with a given territory (which would allow the identification and application of the governing law). The substantive check is difficult to apply in an ubiquitous case as is the use of DLT. Depending on the characterisation of the issue e.g. as a service, a registry, a claim or an IP right, the solutions will materially change, affecting end consumers or investors. In many cases, the rule of conflict of law already exists in the European acquis and national laws, so the intended legislation should consider the already existing solutions to provide consistent application and certainty in terms of jurisdiction. Such a solution could potentially take into account both the registered office of the core service providers and the residence of retail investors

Any failure in the objective of taking care of this international private law aspect, could produce a regulation that would be very easy to circumvent by a variety of actors. These could then opt for regulatory arbitrage without limiting the reach of their business and potentially affect European investors and the European economy and financial stability.

One of the most challenging tasks when dealing with "crypto-assets" will be finding the appropriate regulation that balances the different interests in place, enhancing an adequate and competitive environment.

We would urge the European Commission to ensure that DLT systems can comply with GDPR in a rational and secure way. The immutability of this technology and the impossibility to delete the data, but also the lack of clarity as to what would be enough to comply with a logical (if not physical) deletion is preventing these systems from handling personal data rationally and safely. The need to keep personal data away from the distributed ledger(even if it is a permissioned DLT that guarantees full confidentiality of the data) and subsequently having to keep satellite records in traditional technologies to ensure that the data will be erasable is not contributing to the overall safety of the data, but is rather adding complexity and costs. This results is that even where the DLT is the safest system to guarantee the confidentiality of the data, a whole alternative process and database needs to be implemented. Compliance with GDPR is particularly challenging when personal data needs to be involved in the certification of a transaction in the ledger (e.g. if legal identification of the signatory is required to provide legal validity to the transaction).

Q112 - Have you identified national provisions in your jurisdictions that would limit and/or constraint the effective functioning of DLT solutions or the use of security tokens?

☒Yes

☐No

☐Don't know / no opinion/not relevant

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q112.1 - Please provide specific examples (national provisions, implementation of EU acquis, supervisory practice, interpretation, application…) and explain your reasoning for your answer to question 112.

FESE members have identified that there are cases where national provisions would limit or constraint the effective use of DLT solutions to security tokens, especially related to investor´s rights.

In the first place, FESE considers it crucial that any prospective legislation on "crypto-assets" includes a specific rule for conflicts of law in order to provide certainty as to which law is applicable .

The challenge with "crypto-assets" in this regard stems from the fact that DLT implies multiple locations, meaning that there may not be a single connection with a given territory (which would allow the identification and application of that particular law). The substantive check is difficult to apply in an ubiquitous case as is the use of DLT. Depending on the characterisation of the issue as a service, a registry, a claim or an IP right, the solutions will materially change, affecting end consumers or investors. In many cases, the rule of conflict of law already exists in the European acquis and national laws, so the intended legislation should consider already existing solutions to provide consistent application and certainty in terms of jurisdiction. Such a solution could potentially take into account both, the registered office of the core service providers and the residence of retail investors.

Any failure to handle this international private law aspect could produce a regulation very easy to circumvent by a variety of actors. These could then opt for regulatory arbitrage without limiting the reach of their business, and potentially affect European investors and the European economy and financial stability.

One of the most challenging tasks when dealing with "crypto-assets" will be finding the appropriate regulation that balances the different interests in place, enhancing an adequate and competitive environment.

FESE would urge the European Commission to ensure that DLT systems can comply with GDPR in a rational and secure way. The immutability of this technology and the impossibility to delete the data, but also the lack of clarity as to what would be enough to comply with a logical (if not physical) deletion is preventing these systems to deal with personal data rationally and safely. The need to keep personal data away from the distributed ledger, even if it is a permissioned DLT that guarantees full confidentiality of the data, and subsequently having to keep satellite records in traditional technologies in order to ensure that the data will be erasable is not contributing to the overall safety of the data, but rather adding complexity and costs. This results in the paradox that even where the DLT is the safest system to guarantee the confidentiality of the data, a whole alternative process and database needs to be implemented. Compliance with GDPR is particularly challenging when personal data needs to be involved in the certification of a transaction in the ledger (if legal identification of the signatory is required to provide legal validity to the transaction, for example).

Assessment of legislation for 'e-money tokens'

Q113 - Have you detected any issue in EMD2 that could constitute impediments to the effective functioning and/or use of e-money tokens?

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

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q113.1 - Please provide specific examples (EMD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application…) and explain your reasoning for your answer to question 113:

N/A

Q114 - Have you detected any issue in PSD2 which would constitute impediments to the effective functioning or use of payment transactions related to e-money token?

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

Q114.1 - Please provide specific examples (PSD2 provisions, national provisions, implementation of EU acquis, supervisory practice, interpretation, application…) and please explain your reasoning for your answer to question 114:

N/A

Q115 - In your view, do EMD2 or PSD2 require legal amendments and/or supervisory guidance (or other non-legislative actions) to ensure the effective functioning and use of e-money tokens?

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

Q115.1 - Please provide specific examples and explain your reasoning for your answer to question 115:

N/A

Q116 - Do you think the requirements under EMD2 would be appropriate for "global stablecoins" (i.e. those that reach global reach) qualifying as e-money tokens?

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

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

Q116.1 - Is there any other requirement under EMD2 that would be appropriate for "global stablecoins"?

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

N/A

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80

Q116.2 - Please explain your reasoning for your answer to question 116:

N/A

Q117 - Do you think that the current requirements under PSD2 which are applicable to e-money tokens are appropriate for "global stablecoins" (i.e. those that reach global reach)?

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

Q117.1 - Please explain your reasoning for your answer to question 117:

N/A

Additional information

Should you wish to provide additional information (e.g. a position paper, report) or raise specific points not covered by the questionnaire, you can upload additional documents.

Same business, same risks, same rules

Current regulation should apply, as these pieces of legislation have been established to ensure market integrity as a key learning outcome from the financial crisis. Furthermore, market actors can only develop use-cases, services and invest into innovation provided that there is legal certainty.

Tech-neutrality

It has to be ensured that the principle of tech-neutrality within the regulatory framework is upheld. Regulators should ensure that regulatory requirements are not circumvented by digital infrastructures / DLT. In general, as long as the operator is compliant with the rules the IT-system should not be regarded. However, technology related "new" risks should be taken into account.

Role of FMIs

Technology is an enabler to perform services, e.g. DLT could be seen as an evolution for the financial industry. FMIs (such as exchanges/MTFs, CCPs and CSDs) today provide important functions to markets as proven in and after the financial crisis and will continue to do so in the future. FMIs should explicitly be allowed to handle all forms of "digital assets". However, their roles might change, but the core functions to ensure trust in markets will still be needed in a "new" digital or DLT environment and cannot all be easily performed by new technology only.
A trusted third party is always needed in the financial industry to create trust in the market and is responsible, especially to address the following functions like:

- Control access/admission
- Set rules for the participating nodes
- Address potential conflicts of interest and KYC and AML requirements
- Act as responsible party for regulators /supervisors
- Apply risk management
- Be reliable for market integrity, security and other regulatory requirements.

FESE Avenue de Cortenbergh, 116, 1000 Brussels — info@fese.eu — +32 2 551 01 80