Consultation response

European Commission Public Consultation – An EU Framework for Markets in Crypto-assets

19 March 2020

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on the Public Consultation (referred to hereafter as "the CP") on an EU FRAMEWORK FOR MARKETS IN CRYPTO-ASSETS. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

Our high-level response to the CP is provided below and followed by answers to the individual questions raised.

I. High-Level Response:

AFME welcomes the European Commission (Commission) in bringing forward a comprehensive EU framework for the regulation of crypto-assets that promotes innovation while mitigating risks to consumers, investors, and financial stability.

We propose the following four recommendations to support the development of a fit for purpose European regulatory framework for markets in crypto-assets:

- ***AFME recommends that the Commission publish a more detailed taxonomy on the classification of crypto-assets as a first step in order to provide regulatory clarity for market participants:*** It is important that the Commission clearly differentiates between different types of crypto-assets in order to assign the appropriate regulatory treatment that is calibrated to the risks and level of oversight required. The classification of crypto-assets based on economic function is a useful starting point for providing more regulatory clarity. However, a secondary and more detailed analysis is required to consider the various functionalities of different types of crypto-assets. This analysis is a crucial first step to ensuring the applicable regulatory requirements are suited to crypto-asset related risks.

- ***AFME recommends that the Commission applies existing regulation with any necessary amendments or additional guidance where possible to encourage innovation and foster a level playing field, applying the principle of 'same activity, same risk, same regulation'[1]:*** It is important that the EU regulatory framework remains technology agnostic (to the extent possible)[2] to encourage innovation and foster a level playing field. The use of Distributed Ledger Technology (DLT) to record traditional assets does not necessarily indicate the creation of a new asset, and the Commission should first consider whether a crypto-asset activity is akin to an existing regulated activity, and apply the principle of 'same activity, same risk, same regulation'. In these cases,

[1] e.g. G7 working Group on Stablecoins Report, *Investigating the Impact of Global Stablecoins* (October 2019), p 1 *available at:* https://www.bis.org/cpmi/publ/d187.pdf.

[2] We support the approach taken by the ROEFIG in their report *30 Recommendations on Regulation, Innovation and Finance*, p 12-13 https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf.

we believe existing regulation, with any necessary amendments, should apply. This also should include the applicability of existing regulation to other entities who may be currently outside the regulatory perimeter that conduct the same or similar activities as regulated banks or financial institutions, as there may be significant risks that such activities may entail. To protect investors/consumers, market integrity and financial stability, these entities should also be included where applicable within the regulatory perimeter.

- ***AFME recommends that the Commission provide additional clarification on how existing rules will apply to crypto-assets, as those rules were not originally designed with crypto-assets in mind:*** Firms require additional guidance to clarify how the existing EU financial services regulations will apply to crypto-assets in order to make full use of the functionalities and potential benefits that crypto-assets could offer as they mature. The current regulatory framework was not originally designed with crypto-assets or DLT in mind, as they are based primarily around bilateral relationships rather than the multilateral nature of distributed financial networks. This approach will support the development of a fit for purpose regulatory framework, that can contribute to furthering the objectives of the Digital Single Market (DSM) and Capital Markets Union (CMU).

- ***AFME recommends that the Commission ensures that the EU regulatory framework for crypto-assets is globally aligned, wherever possible, in order to sufficiently mitigate risks:*** A globally aligned regulatory framework is critical for maintaining financial stability and protecting end users, to address gaps in supervision across jurisdictions that could create systemic vulnerabilities as the use and volume of crypto-assets continues to grow. First, any work on a pan-European crypto-asset taxonomy should feed into any on-going global initiatives on classification (e.g. G7/G20, FSB, BIS, IOSCO[3]). Second, there may be a need for global minimum operating and conduct standards for currently un-regulated crypto-asset related activities to protect market integrity as well as the security and privacy of end users.

AFME would welcome the opportunity to discuss our response to this CP in further detail. Specifically, to identify opportunities where AFME can continue to support the European Commission in this important initiative.

Consultation Response

I. Questions for the general public

Q1 – 4 AFME has not responded to these questions.

II. Classification of crypto-assets

Q5 Do you agree that the scope of this initiative should be limited to crypto-assets (and not extended to digital assets in general)? Yes/No/Don't know.

Yes, AFME believes this initiative should focus on the regulation of crypto-assets and exclude the broader category of digital assets and activities. We welcome in particular, a focus on crypto-asset activities that are akin to traditional financial activities, as these crypto-asset activities require further clarity and guidance from the Commission as to how existing regulation would apply.

To help provide clarity for crypto-asset related discussions ongoing at the national and EU level, we request that the Commission provide a common, and uniform, definition of a crypto-asset that can be used by supervisory bodies and the industry.

[3] E.g. *Harmonisation of Critical OTC Derivatives Data (Other than UTI and UPI),* Technical Guidance, BIS, CPMI-IOSCO –(Apr. 2018), *available at*: https://www.bis.org/cpmi/publ/d175.htm

Q6 Would it be appropriate to create a classification of crypto-assets at EU level?

Yes, AFME supports the uniform classification of crypto-assets at the EU level.

We believe a harmonised, pan-European taxonomy for crypto-assets is a crucial first step towards alignment and common understanding. This taxonomy should also be harmonised at a global level. An EU and globally harmonised taxonomy, coupled with the clarification of the applicable rules, would lead to greater regulatory certainty for participants engaged in cross border activity and would encourage innovation. However, we note the potential conflicts of law regarding the classification of crypto-assets in different national jurisdictions across Europe, so we request the Commission to consider how possible fragmentation in the application of a high-level classification (such as the one proposed in this CP) could create additional barriers for market participants.

Q7 What would be the features of such a classification?

AFME, as part of the Global Financial Markets Association (GFMA), is currently developing a detailed approach to the classification and understanding of crypto-assets. We will share this with the Commission, once available, for discussion. We note that the market continues to develop at pace, therefore any definitions used in this response could be subject to change based on future industry and/or regulatory initiatives.

As a general point, we would also like to reiterate that the crypto-asset market is global and cross border, therefore it is important to coordinate a pan-European taxonomy with the work of global organisations such as the Bank for International Settlements (BIS), Basel Committee on Banking Supervision (BCBS), International Organisation of Securities Commissions (IOSCO) and the Financial Stability Board (FSB), to ensure a globally aligned taxonomy.

Q8 Should it distinguish between payment, investment, utility and hybrid tokens? Yes/No/Don't know

Q8.1 If yes, would any further sub classification be necessary?

Q8.2 Please explain

AFME supports the initial classification of crypto-assets based on their predominant economic function (i.e. payment, investment, utility) as an important starting point, and we recognise that there has been significant convergence towards this method of classification within Europe.

However, a secondary and more detailed analysis is required, to consider the various functionalities of different types of crypto-assets, that is adequate to the risks and level of oversight required. This analysis should be completed as a crucial first step to determining: whether a crypto-asset falls within the regulatory perimeter, if so, what the applicable regulatory requirements are, and whether these requirements are suited to crypto-asset related risks. We note that further classification or reclassification may be required as the market continues to develop at pace.

As stated in Q 7 above, we are currently developing an approach to classification and understanding of crypto-assets that considers these factors. We look forward to presenting this to the Commission, once available, for discussion. In the meantime, we provide some initial considerations on a few examples of hybrid tokens below.

Hybrid tokens:

We note two possible examples of hybrid tokens (although there may be others):

1. Crypto-assets that exhibit characteristics of different types of crypto-assets *at the same time:*

   For example, a crypto-asset that contains typical features of a security token and features of a payment token at the same time. In this instance, careful consideration should be taken as to where a crypto-asset is potentially covered by one or more regulatory frameworks, as all respective obligations will need to be satisfied. Regulators should provide further rules or guidance on applicable regulatory obligations and how to apply those obligations (for instance how to calculate the token monetary value to which those obligations apply). Regulators should also address any potential conflicts of laws.

2. Crypto-assets that exhibit characteristics of different types of assets *through time:*

   For example, a crypto-asset that initially has the features of a utility token but then acquires the features of a security token over time (or vice versa). A crypto-asset can also be structured from inception as a hybrid instrument, with contingent changes in instrument categorisation pre-programmed in its coding, based on predefined potential future events (e.g. an automated convertible note)[4].

   In the case of hybrids that change through time, regulators should provide appropriate and clearly defined rules and/or guidance on how to assess when regulatory treatment would change, particularly when the crypto-asset is being traded on a secondary market. This guidance should leverage existing practises in the market today when an instrument changes features; for example, this could include a reassessment at a point where the economic function of a hybrid token undergoes changes or conversion. Should any other types of hybrid tokens develop over time, the treatment of these new crypto-assets should be considered as they develop.

We believe that caution should be exercised against hybrid tokens becoming a 'catch all' category for crypto-assets. This could risk conflating very different types of crypto-assets from a regulatory perspective and make this category difficult to monitor and manage. We wish to avoid the creation of a category that crypto-assets fall within only because they contain new or unique features. A catch-all bucket would create regulatory uncertainty for market participants and limit innovation in this space. Therefore, we request further guidance on the treatment of different types of hybrid tokens currently available to avoid this scenario.

We also request the Commission to continue to collaborate with other international regulators to work towards convergence in the treatment of hybrid tokens at the global level. This is particularly important for international entities, as any variations between jurisdictions would increase the complexity of regulation and raise the cost of compliance.

Further, please see our response to Q 61 for additional details.

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?

Based on preliminary analysis, an account credit-balance recorded on DLT could qualify as a deposit if it were otherwise able to satisfy the definition of a deposit as set out in DGSD Article 2(3). However, this may require further consideration as the current regulatory framework was not originally created with DLT in mind. The regulatory framework should be technology neutral to the use of DLT by regulated deposit taking/credit institutions to evidence or record account credit balances. As far as necessary, this should be further clarified and taken into consideration by the Commission.

[4] See https://media.consensys.net/the-automated-convertible-note-is-a-big-deal-for-blockchain-startups-cc1dd70904fb for more detail.

The nature of deposits should not be altered just because they are represented on DLT. When a regulated bank (or comparable deposit taking/credit institution) uses DLT to evidence account balances, it is simply using a new electronic means of recording an account balance on its books. We believe this method is equivalent to electronic ledger methods that are already widely used in the industry today.

We do not believe the DGSD definition of deposit prescribes the use of a particular technology. The definition and treatment of deposits under DGSD and other core banking regulations should remain technology neutral to encourage innovation and ensure that deposit taking institutions are not disadvantaged by other non-financial competitors.

We note that account credit balances recorded using DLT by a bank (or comparable deposit taking/credit institution) are not considered as crypto-assets under all taxonomies, as they should not be construed to create a new asset class with separate intrinsic value from the funds they represent. However, we have included this in our response to be responsive to varying definitions of crypto-assets under consideration, and to comprehensively articulate when the use of DLT would not require new regulatory treatment but would be governed by an existing regulatory framework.

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

Q10 In your opinion, what is the importance of each of the potential benefits related to crypto-assets listed below? Please rate from 1 (not important) to 5 (very important)

- Issuance of utility tokens as a cheaper, more efficient capital raising tool than IPOs (3)
- Issuance of utility tokens as an alternative funding source for start-ups (2)
- Cheap, fast and swift payment instrument (3)
- Enhanced financial inclusion (3)
- Crypto-assets as a new investment opportunity for investors (3)
- Improved transparency and traceability of transactions (5)
- Enhanced innovation and competition (4)
- Improved liquidity and tradability of tokenised 'assets' (5)
- Enhanced operational resilience (including cyber resilience) (4)
- Security and management of personal data (3)
- Possibility of using tokenisation to coordinate social innovation or decentralised governance (3)

Q10.1 Any benefits missing?

We believe the use of DLT for the provision of crypto-assets should be called out as a specific benefit. DLT has the potential to bring significant benefits to both market participants and consumers, including increased efficiencies at various stages of the capital markets transaction lifecycle (from trading to settlement). DLT can also be used to increase access to certain financial products, drive financial inclusion, improve the resiliency of market infrastructure and change the way market participants interact with one another.

Potential efficiencies include (among others):

- Reduced costs and complexity in using a single ledger "reduces the need for reconciliation and confirmation of trade details between back offices post-trade"[5]
- Improved end-to-end processing speed and availability of assets and funds;

[5] *BIS Quarterly Review,* Bank of International Settlements (Mar 2020), *available at:* https://www.bis.org/publ/qtrpdf/r_qt2003.pdf

- More efficient allocation of capital, which reduces funding costs and improves balance sheet (capital) velocity and treasury / liquidity and collateral management;
- Faster settlement times, reduced trade breaks and reconciliations required, which mitigates counterparty and settlement risk;
- Enhanced regulatory compliance, auditability, and transparency through a secured record of the transactions;
- Enables users of smart contracts to control the decision to automate the payment of interest or dividends[6]; and
- Reduces post trade settlement risk by enabling less use of intraday unsecured credit, including reducing the reliance on multiple intermediaries.

Beyond the efficiencies described above, DLT can improve investor accessibility to certain asset classes through fractional ownership (the process of splitting ownership of an asset into smaller investment requirements). This will enable regulated financial institutions to further provide consumers/investors financial products that align with their capital market needs. It could also aid in increasing financial inclusion, which includes potentially creating the ability to provide end-users with global access to financial products and services without the need for brick and mortar operations.

DLT can also improve resiliency in capital markets infrastructure, by offering a way to securely, accurately and efficiently store information, optimising how information is protected and distributed. The ability to share data across multiple parties is also a key benefit of DLT, which reduces risk of a single point of failure and creates increased transparency where there is a tamper-resistant record of activity.

DLT could have a major impact on the way financial institutions conduct business. DLT can be used as a shared golden source of data for multiple participants that is cryptographically secured and digitally distributed, which would address centralised data base attack and data recovery issues. If governance and identification of participants were appropriately managed, DLT could increase the sharing of information between trusted participants.

DLT can enhance the handling of data between parties, reduce data processing costs, limit disputes or automate the processing of contractual obligations through the use of programmable smart contracts (e.g. for asset servicing or event processing in derivatives), potentially increasing efficiency in financial markets.

One benefit that is missing from above is the efficiencies DLT can bring in relation to information transfer and management for complex operational processes. Examples of these processes include governance, voting and tax processes.

Regarding the points on issuance of utility tokens, we would like to emphasise that if a utility token is used for capital raising, regulators would need to properly assess what rules should apply to that activity and clarify the legal treatment of that token. Further, we note that security tokens could also be used to raise capital, similar to traditional securities. We request the Commission to consider how the fundraising process can be made cheaper for small and medium-sized enterprises (SMEs) whilst continuing to ensure appropriate levels of consumer and investor protection.

Q11 In your opinion, what are the most important risks related to crypto-assets? Please rate from 1 (not important at all) to 5 (very important)

- Fraudulent activities (5)
- market integrity (e.g. price, volume manipulation) (5)
- Investor/consumer protection (5)
- anti-money laundering and CFT issues (5)

[6] *BIS Quarterly Review*, Bank of International Settlements (Mar 2020), *available at:* https://www.bis.org/publ/qtrpdf/r_qt2003.pdf

- data protection issues (4)
- competition issues (5)
- cyber security and operational risks (5)
- taxation issues (3)
- energy consumption (1)
- financial stability (5)
- monetary sovereignty/monetary policy transmission (5)

AFME recognises that despite the significant benefits crypto-assets could provide, there are a range of important related risks. It is important to note that the specific risks associated with a crypto-asset will depend on the type of crypto-asset under consideration. Crypto-assets will carry different risks based on various factors such as the activity the crypto-asset is being used for or the presence of an identifiable issuer. Therefore, the scores provided above are a rough indication; further examination based on the specific risks of different types of crypto-assets will be necessary.

We do note however that anti-money laundering and countering the financing of terrorism (AML/CFT) considerations and potential impacts on financial stability are key priorities for the industry and regulators. We welcome the work of the European Banking Authority (EBA), in consulting on revised guidelines for ML/TF risk factors, where guidelines for retail banks that offer virtual currency services to customers have been proposed[7].

We also note the importance of the risks posed by crypto-assets to consumer/investor protection. Regulated entities who offer crypto-asset services are subject to the full suite of financial services regulations in order to protect end users, the market and financial stability. With this comes a focus on high standards for governance, cyber security and operational resilience. However, there are instances in the crypto-asset market where unregulated entities are offering similar products and services in the EU as regulated entities, whom either fall outside the regulatory perimeter or conduct their activities to other jurisdictions. This is problematic for consumers and investors in the EU, who may not be aware of the different risks associated with these offerings and therefore may be extremely vulnerable to fraud, theft or loss. Therefore, we believe it is necessary that entities involved in crypto-asset activities be treated using the principle of 'same activity, same risk, same regulation'[8], noting that any treatment should be proportionate to the risks arising from the scale and nature of the activity conducted. In addition, the cross-border nature of those activities highlights the need for global cooperation and coordination to ensure a level playing field.

Where DLT networks operate as an infrastructure for the provision of financial services, there may be a need for appropriate operating and governance standards. In some cases, there may be a need for a legal entity to oversee and operate a DLT network to conduct a regulated activity, whom regulatory requirements are assigned to.

Finally, AFME finds that energy consumption is an important issue, particularly when linked to the Commission's sustainability package and an increased focus on the environmental impact of investment. However, energy consumption only represents a significant concern for those crypto-assets that require mining (e.g. bitcoin[9]) not crypto-assets as a whole.

Q12 In your view, what are the benefits of 'stablecoins' and 'global stablecoins'? Please explain.

[7] *EBA Consults on Revised Guidelines on Money Laundering and Terrorist Financing Risk Factors*, EBA (Feb. 05, 2020), *available at*: https://eba.europa.eu/eba-consults-revised-guidelines-money-laundering-and-terrorist-financing-risk-factors

[8] e.g. https://www.bis.org/cpmi/publ/d187.pdf p 1

[9] Bitcoin appeared to account for 75% of total energy consumption in 2018. Other considerations beyond type of protocol are the type of mining equipment used and the energy efficiency of mining data centers, see https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf pages 81-83

We believe any stablecoin arrangement has the potential to become global, and therefore we would not recommend distinguishing between 'stablecoins' and 'global stablecoins'. We request the Commission to instead distinguish between 'stablecoins' and 'systemically important stablecoins', i.e. those stablecoins that have the capacity to impact global financial markets or global financial stability, or incur mass scale adoption. For more detail please see our response to Q 24.

AFME defines a 'stablecoin' as a digital medium of exchange, a means of value transfer, a unit of account, and/ or a store of value using a distributed platform that has a fixed value, or fixed means of calculating, its redemption value, that is not a digital representation of a fiat currency held on account at a bank (or comparable deposit taking/credit institution). We note that there are several possible categorisations depending on their traits, such as their linkage to fiat currency, structuring mechanisms, types of underlying assets, valuation stability, type and levels of collateralisation, asset supply controls, risk management and central hedging. Further, stablecoins could be issued by financial institutions, private companies, or public bodies such as central banks, among other mechanisms. As stated in our response to Q 9, account credit balances recorded using DLT by a bank (or comparable deposit taking/credit institution) should not be construed to create a new asset class or require new regulatory treatment but should be governed by the existing regulatory framework.

Care should be taken by regulators to ensure the principle of 'same risk, same activity, same treatment' is applied to the regulation of stablecoins. We would like to emphasise that additional regulatory oversight should not be applied to existing regulated financial institutions that are 'systemically important' who issue stablecoins that are deemed systemically important. However, firms that are not systemically important but issue stablecoins deemed systemically important, should be held to similar regulatory requirements as systematically important financial institutions (for more detail see our response to Q 24).

Some stablecoins are issued by a recognised issuer and confer redemption rights at either a fixed or variable rate. Typically, asset-backed stablecoins are partially or entirely backed by an underlying asset or asset basket. In general, asset-backed stablecoins should be regulated as the underlying asset. On the other hand, algorithmic stablecoins are created by a protocol that uses smart contracts and implements, among other processes, stabilisation policies and mechanisms in a fully decentralised way to which different entities contribute using decentralised governance.

A globally consistent regulatory approach is needed to provide consistent treatment to the various types of stablecoins. For instance, a stablecoin that is pegged to an underlying basket of currencies (i.e. an index) may be classified and regulated as a security in some jurisdictions or a financial instrument such as a collective investment scheme in others, depending on how the stablecoin is structured. Once a stablecoin that is designed for payment purposes is subject to securities regulations (e.g. prospectus requirements, trading rules and investor protection standards) it may become legally and pragmatically difficult for the stablecoin to continue to be used as a payment instrument.

We request that the Commission continues to collaborate with international supervisors/regulators in the development of the regulatory treatment of stablecoins. This internationally consistent regulatory framework must also be dynamic and flexible to take account of any changes to the regulatory status of a stablecoin over time and the rapid development of the underlying technology.

Third, we find properly constructed stablecoins, or other representations of sovereign fiat currency on a ledger could bring various benefits to wholesale markets, such as faster post trade settlement processes and better cost and capital management, particularly when other parts of the value chain are also digitised. See our response to Q 10 for benefits in using DLT more generally, however we have listed some additional points for increased efficiency below:

- Potentially increased resilience to operational risk through use of a distributed payments system;

- Enabler for the tokenisation of the entire transaction lifecycle: tokenising the cash leg allows for faster settlement of other financial products which have been tokenised, such as stocks or bonds, reducing settlement risk and lowering capital requirements; and
- Providing the ability to conduct transactions outside market hours, possibly 24/7.

We note stablecoin arrangements with systemic importance could help to:

- Better manage FX risk in cross border scenarios through use of a homogenous currency across a region.

Q13 What are the most important risks related to "stablecoins"? Please rate from 1 (factor not relevant at all) to 5 (very relevant factor)

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

Q 13.1 any other important risks?

Q 13.2 Please explain the potential differences in terms of risks between stablecoins and global stablecoins

It is important to note that the specific risks associated with a stablecoin will depend on the type of stablecoin under consideration. Stablecoins will carry different risks based on various factors such as the structuring of a stablecoin or the presence of an identifiable issuer. Therefore, the scores provided above are a rough indication; further examination of the specific risks of different types of stablecoins will be necessary.

As stated in our response to Q 12, we believe any stablecoin arrangement has the potential to become global, so we recommend the Commission to instead differentiate between 'stablecoins' and 'systemically important stablecoins', i.e. those stablecoins that have the capacity to impact global financial markets or global financial stability, or incur mass scale adoption. Please see our response to Q 12 for regulatory approach to systemically important stablecoins and for more detail please see our response to Q 24.

We encourage a continued analysis of the risks around the structure and various features of stablecoins. For example, with asset-backed stablecoins there are risks related to inappropriate custody and management of the underlying assets and issues related to the structuring of the stablecoin, their stabilisation mechanisms and/or levels of collateralisation (among other characteristics). There may also be a risk of legal uncertainty unless it is clarified that stablecoins are under scope/fungible in a similar manner to traditional payment instruments with similar characteristics and that there is clear finality of payment or settlement when using stablecoins.

In most cases, the value of asset-backed stablecoins is linked directly to the value of the underlying assets, and how those underlying assets are held and protected. Therefore, we request the Commission to ensure that issuers of these stablecoins and the underlying structure to hold those assets backing the stablecoins are regulated to protect the integrity

of financial markets and consumers. Consideration should be given to how existing regulatory frameworks would apply. This includes the rights and entitlements of stablecoin holders to access or redeem the underlying assets, ensuring that underlying assets are adequately segregated, not comingled with own funds from the stablecoin issuer, are adequately protected from misappropriation, audited and that the issuer complies with appropriate capital requirements based on the activity performed and the risks involved.

Further, where stablecoins are linked to fiat currency and issued by an institution that is not a regulated credit institution, there are risks related to how the underlying fiat currency is kept and/or invested and what protections (such as deposit insurance) apply. Care should be taken to regulate these types of stablecoins in alignment with current regulatory frameworks.

We would like to add that there are risks to investors, consumers and potentially financial stability generally in cases where there are gaps in the applicability regulation to unregulated entities that provide stablecoin services – for more detail see our response to Q 11. Regarding energy consumption, also see our response to Q 11.

As with all new technologies and digitisation more broadly, regulatory agencies and firms should continue to assess any possible additional risks, such as cyber and operational risks, and reflect that analysis in the risk assessments of crypto-assets and the activity surrounding those crypto-assets.

Q 13.1 We reference here the recent report of the G7 Working Group on Stablecoins[10] who found that stablecoins, regardless of size, pose risks relating to:

- Legal certainty;
- Legal characterisation;
- Technological neutrality;
- Sound governance;
- Financial integrity (AML/CTF);
- Cybersecurity and operational risk;
- Market integrity;
- Data protection;
- Consumer/investor protection; and
- Tax compliance

The G7 Working Group on Stablecoins found that stablecoins that reach global (systemic) scale could pose challenges and risks relating to monetary policy, financial stability, personal data privacy, the international monetary system and fair competition. They consider that when a stablecoin becomes global, some of the risks listed above can become amplified, which in turn runs the danger of transmitting effects to the real economy, with potential consequences on the effectiveness of monetary policy. Therefore, we believe it is important that central banks have a coordinated policy with respect to stablecoins, and we support the report's findings that public authorities should coordinate to ensure a globally consistent response.

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. Please explain.

[10] *Investigating the Impact of Global Stablecoins*, G7 Working Group on Stablecoins (Oct. 2019), *available at:* https://www.bis.org/cpmi/publ/d187.pdf

AFME finds that a bespoke regime at EU level for crypto-assets not currently covered by EU financial services legislation (such as cryptocurrencies) could support the development of certain segments of the crypto-asset ecosystem that abides by specific minimum standards. This would provide greater regulatory certainty for market participants. We emphasise however that this "bespoke regime" should be based on the use of existing principles first (e.g. on consumer/investor protection, market integrity, financial stability, etc.) to address the risks identified in a proportional way, rather than create entirely new regulation at the outset. This includes applying the principle of 'same activity, same risk, same regulation'. The introduction of new risks should only be addressed separately through bespoke regulations in those cases where amendments to, or clarification of, existing rules are not possible or effective to address those risks. For more detail see our response to Q 16.

If bespoke regulation applies to entities that are already regulated in their provision of traditional financial services (such as broker dealers or banks) regulators should ensure this does not create uncertainty or operational inconsistency to the application of regulation when conducted without using crypto-assets.

In the absence of a unified EU regime for those crypto-assets currently outside of the regulatory perimeter, there is a risk that either fragmentation occurs, where national regulators develop their own approach to regulation (increasing the complexity of cross-border activity), or that there is no applicable regulation to cover those crypto-assets. Either scenario would discourage regulated entities from conducting business or innovating in this area. Further, if volumes were to increase significantly and the activity were to be concentrated on unregulated entities, this could create financial stability issues and have spill over effects into existing financial services infrastructure, which may have direct or indirect exposure to those unregulated entities. Therefore, a coordinated and common pan-European approach would reduce fragmentation, promote wider harmonisation, and address potential financial stability issues.

Finally, it is important that any EU regulatory framework (either current or expanded) remains technology agnostic (to the extent possible), risk-based, proportionate and future proof in order to encourage innovation and foster a level playing field. Any possible additional risks, such as cyber and operational risks, should be reflected in ongoing risk assessments.

Q15 What is your experience (if any) regarding national regimes on crypto-assets? Please indicate which measures in these national laws are, in your view, an effective approach to crypto-assets regulation, and which ones are not.

AFME encourages national regulators to take a consistent approach when bringing crypto-assets under the regulatory perimeter to allow their safe development at scale.

We support an approach that looks first to apply existing regulation to crypto-asset activities that are equivalent to currently regulated activities, following the principle of 'same activity, same risk same regulation'. For example, where a regulated bank is undertaking crypto-asset related activity, existing banking regulations should be used as the starting point for understanding whether they are sufficient to address the risks of the activity. This approach can also be used to assess whether existing regulation could be applied to other entities participating in the same activity, who are exposed to the same risks. We believe that bespoke regulations should only be used to address new risks where amendments or clarifications to existing rules cannot effectively address those risks.

We welcome the issuance of guidance with clear expectations for market participants to follow and the use of referencing use-case examples, to make it easier for market participants to understand in practise how regulations would apply.

Q16 How would it be possible to ensure a bespoke regime for crypto-assets/service providers is appropriate to induce innovation while protecting users. Please indicate if such a bespoke regime should include the abovementioned categories (payment, investment and utility tokens) or exclude some of them, given their specific features (e.g. utility tokens).

AFME finds that it would not necessarily be appropriate to capture all types of crypto-assets in a bespoke regime. This decision should be based on the activities that are being conducted, what actors are involved in the transaction, the predominant use of the crypto-asset and whether there is a claim on the issuer.

For instance, unregulated crypto-assets that are used purely for utility purposes (for instance to provide access to non-financial products or services within a closed network) and that are not transferrable outside the network they were created in, would not need to be captured by the regulatory perimeter.

A bespoke regime should leverage existing global standards and principles (for instance relating to consumer/investor protection, market integrity, financial stability, etc.) that have been established by global bodies such as the BIS, FSB and IOSCO, to address the identified risks proportionately. For instance, AFME welcomes the IOSCO consultation report on *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*[11] and generally supports the application of the IOSCO and the Committee on Payments and Market Infrastructures (CPMI) PFMIs to crypto-asset service providers whenever applicable in order to protect end users (including their privacy and security), market integrity and financial stability.

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/No opinion/Not relevant

Q 17.1 If yes, please indicate how this clarity should be provided (guidance, EU legislation), and please explain your reasoning.

AFME agrees that there is a need for greater clarity regarding the prudential treatment of financial institutions' exposures to crypto-assets. For more detail please see the GFMA response to the BCBS Discussion Paper on Designing a Prudential Treatment for Crypto-assets.

Q18 Should harmonisation of national civil laws be considered to provide clarity on the legal validity of token transfers and the tokenisation of tangible (material) assets?

AFME supports where possible the harmonisation of national civil laws to provide clarity on the legal validity of token transfers and the tokenisation of tangible assets. An important aspect of providing regulatory certainty is ensuring that regulation is linked to legal clarity. Specifically, clarity with respect to the legal validity and enforceability of transfers for network participants and third parties is required, including the concept of finality.

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

[11] *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*, Consultation Report CR02/2019, Board of the IOSCO (May 2019), *available at:* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf.

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?

Many of the crypto-assets service providers are involved in more than one of the activities mentioned above. For example, there is nothing to prevent a single entity from acting as a broker, market marker, insurance provider, trading platform, wallet provider and derivative provider.

Within the traditional market infrastructure, the activities referenced above are generally segregated and performed by different entities for good reason. The conflict of interest inherent in allowing an entity to provide several (if not all) of the above services warrants regulatory oversight. Consensus price testing services that cover different types of crypto-assets provide one illustration. As these types of services are used for independent price verification, the calculation of prices should not be performed by entities executing market making or price setting activities. Crypto-assets may enable streamlining some of these functions in a safe, but more efficient way. However, these activities should be examined as they are developed so that any risks can be identified and mitigated.

There are also new possible entities that do not exist in the traditional infrastructure, such as node validators or transaction validators. In some cases, the provision of these services is purely technical. In other cases, these validators perform key activities in the ecosystem, such as confirming transactions, recording ownership or providing a notary function, which may or may not be technical in its essence. Where these activities take place, the performance of the activities should be carefully considered before being subject to similar requirements to those imposed on traditional actors performing similar types of activities. However, we also seek clarification around definitions and various other points of clarification around market participants who perform these types of roles throughout this CP. For example, please see our response to Q 88.

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? Please explain. Yes/No/Don't know no opinion not relevant

We find that if issuers or sponsors of crypto-assets marketed to EU investors/consumers are subject to authorisation and the appropriate regulation and supervision, there should be no need for these entities to have a physical presence in the EU. This is because crypto-assets are decentralised in nature and may operate across borders. Therefore, requiring a physical presence in the EU may be problematic in that there may be a risk in penalising those providers based in the EU by imposing such requirements.

The European regime should seek to prevent against the marketing of crypto-assets in the EU by unregulated providers that are located outside of the EU and are not subject to comparable Know Your Customer (KYC) and AML/CFT standards, so appropriate regulation should for instance include comparable KYC and AML/CFT standards (amongst other requirements).

Q21 Should an issuer or a sponsor of crypto-assets be required to provide information (e.g. through a 'white paper') when issuing cryptoassets? Yes/No/ It depends on the nature of the crypto-asset (utility, payment, hybrid…)

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

AFME supports leveraging existing regulatory frameworks as a starting point. We are of the view that all information that is necessary to evaluate the attributes of and the risks associated with the crypto-asset should be provided by the issuer.

This information should be appropriate to the nature of that particular crypto-asset and proportionate to the risk of that asset as it relates to traditional financial activity and required disclosures (e.g. prospectuses and other regulatory filings). As such, disclosures may not be appropriate or beneficial in all cases, in line with current regulatory requirements.

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

- The consumer rights directive (4)
- The E-Commerce Directive (4)
- The EU Distance Marketing of Consumer Financial Services Directive (4)

22.1/2 Any other requirements not mentioned that issuers should be subject to? 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 and indicate the type of clarification (legislative/non legislative) that would be required.

AFME finds that the nature and form of disclosure should be appropriate for the nature and purpose of that crypto-asset, and crypto-assets equivalent in underlying risks and activity to traditional assets should continue to be regulated in a similar fashion as outlined in the current regulatory framework.

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? (1 - 5 relevance)

- The managers of the issuer or sponsor should be subject to fitness and probity standards (5)
- The issuer or sponsor should be subject to advertising rules to avoid misleading marketing/promotions (5)
- "Where necessary, the issuer or sponsor should put in place a mechanism to safeguard the funds collected such as an escrow account or trust account" (5)

23.1/2 Any other requirements needed? Please explain.

AFME finds that conflicts of interest requirements are needed in order to mitigate any risks to market integrity – see our response to Q 19. The nature and form of disclosure should be appropriate for the nature and purpose of that crypto-asset, and crypto-assets equivalent in underlying risks and activity to traditional assets should continue to be regulated in a similar fashion as outlined in the current regulatory framework.

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.

AFME supports that the regulation of stablecoins, and all other types assets falling under the term 'crypto-assets', should be proportional to the risks involved. We note that any stablecoin arrangement has the potential to become global, therefore we would not recommend distinguishing between 'stablecoins' and 'global stablecoins', but rather we request the Commission to instead distinguish between 'stablecoins' and 'systemically important stablecoins'. The proportionality of risk will need to primarily consider:

- Whether the initiative is predicated upon an existing, large and/or cross-border customer base that is likely to enable rapid scalability;
- The nature of the issuer and its footprint (e.g. is the issuer a regulated deposit-taking institution or otherwise);

- The volume of estimated transactions;
- The number of currencies/securities and countries involved; and
- The underlying composition of the value references of the stablecoin (e.g. is reference value of the stablecoin an index of multiple sovereign currencies).

Therefore, we recommend that stablecoins be continuously monitored by regulators/supervisors, that roles and responsibilities for monitoring are set out and agreed upon and that objective criteria regarding the differentiation between 'stablecoins' and 'systemically important stablecoins' are also aligned.

AFME notes that care should be taken by regulators to ensure the principle of 'same risk, same activity, same treatment' is applied to the regulation of stablecoins. We also note that additional regulatory oversight should not be applied to existing regulated financial institutions that are 'systemically important' who issue stablecoins that are deemed systemically important. However, firms that are not systemically important but issue stablecoins that are deemed systemically important should be held to similar regulatory requirements as systematically important financial institutions. Please also see our answer to Q 12.

Q25 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 if each proposal for stablecoins is relevant or not relevant.

- The reserve of assets should only be invested in safe and liquid assets (such as fiat-currency, short term-government bonds, ...) (Relevant)
- 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 (Relevant)
- The assets or funds of the reserve should be segregated from the issuer's balance sheet (Relevant)
- The assets of the reserve should not be encumbered (i.e. not pledged as collateral) (Relevant)
- The issuer of the reserve should be subject to prudential requirements rules (including capital requirements) (Relevant)
- "The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating" (Relevant)
- "Obligation for the assets or funds to be held in custody with credit institutions in the EU" (Not relevant)
- Periodic independent auditing of the assets or funds held in the reserve (Relevant)
- 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 (Relevant)
- "The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically" (Relevant)
- "Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer" (Relevant)
- "Obligation for the issuer to use open source standards to promote competition" (Relevant)

25.1/2 Any other requirements not mentioned that could be imposed on issuers/managers of reserve? Please explain.

As a general principle, any crypto-asset should be regulated as the electronic form of any underlying asset, using the principle of 'same risk, same activity, same regulation'. For more detail see our response to Q 12 and 24. There is a need

to differentiate credit balances recorded using DLT by a bank from crypto-assets (including stablecoins). The ranking below applies to stablecoins only and not to traditional depositary products evidenced by DLT, to which existing deposit regulations should continue to apply.

AMFE supports the imposition of requirements similar to those in funds, such as the segregation of duties and valuations of the reserve. Regarding valuations of the reserve, trusted and reliable market data and auditability will be required, for instance, if a stablecoin is pegged to a currency. We also support leveraging existing frameworks that would apply when a financial market participant handles reserves or assets that serve as underlying value.

Transparency around calculations and the appropriateness of governance structures should also be clearly identified for both users and supervisors, as well as details on any banding or collaring. Other arrangements that may enhance confidence and reliability include clarity on the settlement finality, redemption and exit mechanism for the holders, and arrangements between issuers and distributors that guarantee convertibility, especially where stablecoins are paired with appropriate governance and transparency around the reserve function.

Further, we find that all of the above listed criteria should apply to all issuers/managers of the reserve with the exception of the following:

- "*Obligation for the assets or funds to be held in custody with credit institutions in the EU".* We do not see any justification for mandating custody of the same be performed by a credit institution or an EU entity. This proposed requirement would impose more restrictions on the custody of the assets underlying the stablecoin than the requirements that currently exist for the custody of traditional assets. For example, preamble 34 of the Alternative Investment Fund Managers Directive (AIFMD) states: the depositary should be a credit institution, an investment firm or another entity permitted under Directive 2009/65/EC, given the importance of the custody function. For non-EU AIFs only, it should also be possible for the depositary to be a credit institution or any other entity of the same nature as the entities referred to in this recital as long as it is subject to effective prudential regulation and supervision which have the same effect as EU law and are effectively enforced. Therefore, we recommend that the requirement is reworded to state: "obligation for the assets or funds to be held in custody by a regulated entity";

- *"The value of the funds or assets held in the reserve and the number of stablecoins should be disclosed periodically".* We do not believe this is relevant if the periodic auditing of the issuer provides this information. Therefore, the periodic audit should suffice in this regard; and

- *"Requirements to ensure interoperability across different distributed ledgers or enable access to the technical standards used by the issuer"*. This would be a difficult requirement to impose based on the limitations of innovation but should be encouraged.

Regarding the requirement *"The issuer and the reserve should be subject to specific requirements in case of insolvency or when it decides to stop operating",* we note that there should be clear rules set out for regulators and investors on the seniority of claims in the event of an insolvency (e.g. whether the shareholders of the issuer get reimbursed before the coin holders or vice versa). These rules should align with and be based on current regulations around equivalent monetary instruments.

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

Yes, AFME requests the Commission to consider the regulatory treatment of retail and wholesale stablecoins, based on the activity the stablecoin is being used for and the risks associated with that activity. For instance, there are cases where wholesale stablecoins are used to facilitate transactions between wholesale providers, whereas retail stablecoins can be used to facilitate transactions for a larger range of users.

We support that in using the principle 'same activity, same risk, same regulation', the purchasing rules for wholesale vs. retail stablecoins should be proportionate and related to the different risks that each activity entails. Further, it is important that regulators consider how the user of the stablecoin should be treated and whether the issuer is already covered by appropriate regulation that would also cover the performance of these activities.

Q27 – 30 AFME has not responded to these questions.

Q31 In your opinion what are the main risks in relation to custodian wallet service provision? Please explain (1 completely irrelevant – 5 highly relevant)

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

31.1/2 Any other risk you would foresee? Please specify and explain.

We believe the same regulations that apply to regulated entities that act as custodian of money or financial instruments should apply also to other players when delivering these services.

Custody of all types of crypto-assets broadly relies on the safekeeping of the asset and possession of private keys. There is a large spectrum of safekeeping options when it comes to the custody of crypto-assets, such as hot and cold storage. We request the Commission to consider the different risks of these options in more detail. Some of the risks are outlined below.

Risks to investors/consumers
One key risk to investors/consumers is the fact that the regulatory framework currently does not cover all types of crypto-asset custodians. Today, entities who provide custody of traditional securities and money are covered by the existing regulatory framework, for example, the Markets in Financial Instruments Directive (MiFID), AIFMD and Undertakings for the Collective Investment in Transferable Securities (UCITS). Where a cryptoasset meets the definition of a financial instrument or other already existing regulatory classification such as e-money or a deposit, safekeeping activities performed by custodian wallet providers would fall within this regulatory framework.

However, entities (such as cryptocurrency custodian wallet providers) that provide third party crypto-asset custody services for unregulated crypto-assets are not covered by these existing frameworks. This has resulted in a situation where regulated and unregulated custody service providers are offering the similar products and services, but consumers are unlikely to be aware that the service offerings provide different levels of protection.

To ensure the risks identified above are mitigated, we believe all entities who provide third party crypto-asset custodian services should be supervised (noting that consideration will need to be given to the appropriateness and applicability of the existing regulatory regimes, which are currently relevant when acting as a custodian for financial instruments, in the context of providing custodial wallet services.). The appropriate requirements and level of supervision will depend on the type of crypto-asset held in custody. Although there is no global or uniform definition of the term custody, we support minimum standards for custody, which could include:

- Asset maintenance;
- Segregation and security; appropriate management and keeping of assets to prevent loss or damage;
- Controls to ensure assets are not misappropriated by persons with access to them; and
- Segregation of assets between clients.

Systemic risks
We note that bankruptcy of a large custodial wallet provider could also pose a systemic risk to the industry if it were to be significantly interconnected, however this would only be the case if the assets are not properly segregated. The primary systemic risk relates to an operational or cyber security failure that compromises the assets in safekeeping. This could be the case with either a custodian service provider or a wallet provider.

Loss or theft of certain crypto-assets (i.e. cryptocurrencies)
Some cryptocurrencies that are not yet covered by existing custody rules behave like cash in that they lack traceability and reversibility that would allow the reversal of fraud, loss or theft. Therefore as with custodians of cash, custodians of these crypto-assets should provide adequate controls and investor protection to their clients in case of fraud, loss or theft. Further, in instances where a custodian has limited controls or where there are flaws in the systems or software used, the loss or theft of a substantial amount of a single crypto-currency based on errant transactions or loss of a private key could have a negative impact on consumers.

As a separate point, we request the Commission to clarify its definition of a 'wallet provider' and 'custodian', as we note these entities are not one in the same.

Q32 What are the requirements that could be imposed on custodian wallet providers in order to mitigate those risks? (1 – 5 highly relevant)

- Custodians should have a physical presence in the EU (1)
- Should be subject to governance arrangements, including operational resilience and ICT security (5)
- Should segregate assets of users form those held on own account (5)
- Should be subject to conflicts of interest rules (5)
- Should keep appropriate records of users holdings and transactions (5)
- Should have an adequate complaints handling and redress procedure (5)
- Should be subject to capital requirements (5)
- Subject to advertising rules (4)
- Subject to minimum conditions for contractual relationship with consumers investors (5)

32.1/2 Any other requirements? Please indicate if requirements should be different depending on the type of crypto-asset in custody

AFME finds that the above risks are as relevant for the custody of all types of crypto-assets as they are for the custody of traditional assets, with the exception of the need for custodians to have a physical presence in the EU. It is unclear to AFME what risk would be mitigated through the imposition of this requirement, as long as the custodian is appropriately regulated.

The realities of the crypto-asset provider landscape are such that it is increasingly common for digital services to be provided in a country without a physical presence in the same. The benefits afforded to consumers as a result are clear; limiting the choice available to consumers could prevent them from using the best service available. Whilst mitigating the risks identified throughout this paper through regulation is key, it would seem possible to do so without imposing geographical limitations on the provision of a borderless digital service.

As a general point, activities related to the custody of traditional securities and money is covered by the existing regulatory framework, for example, MiFID, AIFMD and UCITS. As highlighted above, where a crypto-asset meets the definition of a financial instrument or other already existing regulatory classification such as e-money, safekeeping activities performed by custodian wallet providers would fall within the applicable regulatory framework. AFME recommends that the EU regulatory framework follows the principle of 'same activity, same risk, same regulation' to apply equivalent requirements to crypto-asset custodians. For instance, we note that capital requirements for custodians should be equivalent to those that are required for traditional custodians.

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.

Yes, AFME believes where crypto-assets fall within the regulatory perimeter, custodian wallet providers should be authorised to provide custody for all crypto-assets (including those that qualify as financial instruments under MiFID II), when they are able to fulfil the applicable regulatory requirements for safekeeping (for financial instruments this would include MiFID, AIFMD, and UCITS). In this case it is important that there is a clear classification on what kind of crypto-asset is being held in custody. If/how a crypto-asset falls within the regulatory perimeter will determine what kind of requirements a custodian should fulfil in order to be authorised, so our answer to this question will depend on what type of crypto-asset is being considered, and therefore what kind of requirements must be fulfilled to meet authorisation requirements (see our response to Q 31 regarding minimum requirements for all third party custodian services).

In addition, the regulatory perimeter should be extended so that any provider of custodial wallet services for safekeeping of crypto-assets is subject to the same regulatory framework, oversight and licensing/permissioning requirements as custodians of traditional financial instruments. However, the appropriateness and applicability of the existing regulatory regimes which are relevant when acting as a custodian for financial instruments should be explored in detail in the context of providing custodial wallet services, as it is possible that operational differences between crypto-assets and non-crypto-assets may change the way in which regulation applies. For example, there could be differences in the way that systems and controls requirements may apply.

For illustrative purposes, the obligation of a custodian to maintain an independent record of its clients' accounts which can be used as an audit trail, may not be able to be directly applied. By definition, distributed nodes are not independent of each other, so while it is possible that the distributed ledger itself would form part of that audit trail, consideration should be given as to what, if any, additional measures a custodian's records might require to be sufficient and maintain independence from a technological separation perspective.

Q34 Are there certain business models or activities /services in relation to digital wallets (beyond custodial wallet providers) that should be in the regulated space?

AFME finds that any crypto-asset services whereby the provider has access to the private key should be considered in scope, as well as other related ancillary activities such as acquiring services, onboarding and payments. We also find that in-wallet credit provision services and wallet/portfolio accounting valuation should be included. Regarding asset-backed or securities tokens, AFME believes there should be equivalent rules indicating what issuers of securities/funds would be subject to (e.g. transparency of listing, immobilisation/ringfencing/holding on trust of underlying assets, etc.).

Q 35 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 1 completely irrelevant to 5 highly relevant.

- Reception and transmission of orders in relation to crypto-assets (5)
- Execution of orders on crypto-assets on behalf of clients (5)
- Crypto-assets portfolio management (5)
- Advice on the acquisition of crypto-assets (5)
- Underwriting of crypto-assets on a firm commitment basis (4)
- Placing crypto-assets on a firm commitment basis (4)
- Placing crypto-assets without a firm commitment basis (4)
- Information services (an information provider can make available information on exchange rates, news feeds and other data related to crypto-assets) (4)
- Processing services, also known as 'mining' or 'validating' services in a DLT environment (e.g. 'miners' or validating 'nodes' constantly work on verifying and confirming transactions) (3)
- Distribution of crypto-assets (some crypto-assets arrangements rely on designated dealers or authorised resellers) (4)
- Services provided by developers that are responsible for maintaining/updating the underlying protocol (3)
- Agent of an issuer (acting as liaison between the issuer and to ensure that the regulatory requirements are complied with) (5)
- Settlement of orders in relation to crypto-assets (4)

35 1/2 Please illustrate your response to question 35 by underlining the potential risks raised by these services if they were left unregulated and by identifying potential requirements for those service providers

AFME agrees that the above services should be subject to existing or similar requirements that regulated financial institutions are subject to when performing similar activities with similar risks. For instance, regulated institutions leverage code and protocols, developed by third parties and internally, in current financial markets today. Similar frameworks that govern those instances should apply.

We note that there could be new entities that do not exist in the traditional infrastructure, such as node validators or transaction validators. In some cases, the provision of these services is purely technical. In other cases, those validators perform key activities in the ecosystem, such as confirming transactions, recording ownership or providing a notary function, which may or may not be technical in its essence. Where these activities take place, the performance of the activities should be carefully considered before subjecting similar requirements to those imposed on traditional actors performing analogous or similar types of activities. However, AFME also seeks clarification around definitions and

various other points of clarification around market participants who perform these types of roles throughout this CP. For example, please see our response to Q 19 and 88.

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/Don't know.

AFME finds that the rules currently contained in the Second Payment Services Directive (PSD2) should apply, however caveats or separate regulation may be required. We also request clarification from the Commission on whether crypto-assets will fall within the definition of PSD2 transactions, as currently it is unclear how crypto-assets may fall within the regulatory perimeter in this regard.

To elaborate, currently the Fifth Anti-Money Laundering Directive (AMLD5) (recital 10) reflects the EBA's conclusion that virtual currencies should not be confused with 'electronic money' within the scope of the Second E-Money Directive (EMD2) or 'funds' within the scope of PSD2. As reported by the EBA last year, crypto-assets are not banknotes, coins or scriptural money[12]. For this reason, crypto-assets do not fall within the definition of 'funds' set out in point (25) of Art. 4 of the PSD2 unless they qualify as 'electronic money' for the purpose of the EMD2.

Should a firm propose to carry out a 'payment service' using DLT as listed in Annex I to the PSD2 (such as the execution of payment transactions, including issuing 'payment instruments' and/or acquiring payment transactions and money remittance) with a crypto-asset that qualifies as 'electronic money', this activity would fall within the scope of the PSD2 by virtue of being 'funds'. Because the term 'crypto-asset' is broad, which may or may not include assets that are used for payment transactions, of which may or may not fit under the definition of 'electronic money', AFME requests that the Commission clarify whether the crypto-assets described in this response would fall under the PSD2 regulatory perimeter. In any event, AFME advises against the blanket application of EMD2 or PSD2 to crypto-assets more broadly, supporting further assessment as to whether such regulatory perimeters apply to a crypto-asset based on its economic function, its risk-profile, and within the framework as mentioned in the introduction of this response.

C. Horizontal questions

Q37 In your opinion, what are the biggest market integrity risks related to the trading of crypto-assets? (1 completely relevant – 5 highly relevant)

- Price manipulation (5)
- Volume manipulation (wash trades) (5)
- Pump and dump schemes (5)
- Manipulation on the basis of quoting and cancellations (5)
- Dissemination of misleading info by the crypto-asset issuer or any other market participants (5)
- Insider dealings (5)

Q 37.1/2 any other big risk related to trading you would foresee? Please specify, please explain.

It is important to note that the specific market integrity risks associated with a crypto-asset will depend on the type of crypto-asset under consideration. Crypto-assets will carry different market integrity risks based on various factors such as the activity the crypto-asset is being used for or the presence of an identifiable issuer. Therefore, the scores provided

[12] *Report with Advice for the European Commission on Crypto-assets*. EBA Report, p. 14 (Jan. 9, 2019), *available at*: https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf

above are a rough indication; further examination of the specific market integrity risks of different types of crypto-assets will be necessary.

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

Ensuring market integrity is of utmost importance, and there are already principles and controls in place in the traditional financial markets that can and should be made applicable to crypto-asset markets. For example, AFME supports IOSCO's findings in its Final Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (CTP), which consider potential issues relating to market integrity and fairness for a CTP dealing in crypto-assets[13].

Regarding market integrity, the report notes, 'a key consideration for regulatory authorities is the applicability of existing rules relating to market abuse and the capacity of CTPs to prevent and/or detect market abuse'[14] . Further, it notes 'the regulator should assess the reliability of all the arrangements made by the operator for the monitoring, surveillance and supervision of the exchange or trading system and its members or participants to ensure fairness, efficiency, transparency and investor protection, as well as compliance with securities legislation'[15].

The report also notes however that there are new challenges regarding the monitoring of trading on CTPs, for instance where 'new forms of manipulation may occur', or where there are 'unique issues relating to crypto-assets, such as the high price volatility of crypto-assets relative to traditional financial assets, the possibility of trading 24 hours a day and the lack of consistent and stable sources of crypto-asset pricing to support market surveillance systems and activities'[16]. Therefore, we encourage the Commission to consider how existing frameworks can be adapted or enhanced to effectively mitigate these risks. In particular, we note that there should be requirements for exchanges relating to due diligence and KYC to the same extent as would be expected for other asset classes or similar market activity.

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. If yes, please explain how you would see this best achieved in practise.

We request clarification from the Commission regarding the scope of this question, as the need to formally identify the parties will depend on the type of crypto-asset and whether this crypto-asset falls inside or outside the regulatory perimeter. It will also depend on the type of identification required (e.g. does this relate to AML/CFT obligations, MiFID transaction reporting requirements or licensing requirements). In cases where a crypto-asset does fall within the regulatory perimeter and there is a need to formally identify parties, different approaches may be possible for different types of crypto-assets.

Regarding AML/CFT obligations, please see our response to Q 41-46. Regarding MiFID reporting requirements please see our response to Q 59-76.

We note that consideration should be given to compliance with the Financial Action Task Force (FATF) Travel Rule for peer-to-peer transactions.

[13] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf
[14] *Id.* p 20
[15] *Id.*
[16] *Id.*

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?

AFME has not responded to this question.

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

Q 41 Do you consider it appropriate to extend the existing "virtual currency" definition in the EU AML/CFT legal framework in order to align it with a broader definition (as the one provided by the FATF or as the definition of "crypto-assets" that could be used in a potential bespoke regulation on crypto-assets)? Yes/No/Don't know. Please explain.

AFME considers it appropriate to extend the existing definition of 'virtual currency' in the EU AML/CFT legal framework to align it with the FATF terminology of 'virtual assets'. Alignment of regulatory frameworks across the EU would aid the creation of a common global crypto-asset taxonomy that should be underpinned by a common understanding of terms. It should be clarified that 5AMLD will apply to crypto-assets used for payment and investment purposes, namely the categories outlined by the FATF as 'virtual assets'. This would ensure all relevant types of crypto-assets are brought within the regulatory perimeter of the 5AMLD framework, ensuring a level playing field, mitigation of potential risks (including consumer/investor risks, market integrity risks and financial stability risks), greater market transparency and consumer/investor protections across the crypto-asset market.

Q 42 Beyond fiat-to-crypto exchanges and wallet providers that are currently covered by the EU AML/CFT framework, are there crypto-asset services that should also be added to the EU AML/CFT legal framework obligations? Yes/No/Don't know. If you think there are crypto-asset services that should also be added to the EU AML/CFT legal framework obligations, describe the possible risks to tackle:

AFME believes that AML/CFT obligations should apply to crypto-asset exchange services that deal in what is outlined by the FATF as 'virtual assets'. In line with the FATF Guidance on virtual assets and virtual asset service providers (VASPs), an adequate VASPs risk assessment must take into account all of the following risk factors 'types of services, products, or transactions involved, customer risk, geographical factors, and type(s) of virtual asset exchanges'[17]. We also view that cyber risk policies and anti-fraud controls of VASPs should be examined to complete the risk assessment.

In our view, apart from fiat-to-crypto exchanges and wallet providers, the AML/CFT framework should also cover participation in and provision of financial services related to an issuer's offer and/or sale of virtual assets, operation of a machine which utilises automated processes to exchange crypto-assets for money or money for crypto-assets (e.g. crypto-asset ATMs), peer-to-peer exchanges, and crypto-to-crypto service providers that deal in virtual assets and can operate without a central authority facilitating transactions. Many decentralised exchanges require less personal information from their members and crypto-to-crypto providers are not currently mandated to conduct KYC checks in all jurisdictions. Identification and assessment of potential ML/TF risks is impossible without all the necessary information to conduct due diligence.

Further, we would like to clarify that while some wallet providers are already covered by the AML/CFT framework, there is an important distinction to be made between provision of wallet services and provision of custody services for crypto-

[17] *Virtual Assets and Virtual Asset Service Providers*, *Guidance for a Risk-based Approach*, FATF, p. 11 (Jun. 2019), *available at:* https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf (hereinafter the "FATF Report")

assets. For instance, 5MLD defines a custodian wallet provider as 'an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies', which is a limited service which may or may not fall within the regulatory perimeter. In comparison, provision of custody services would typically be understood to imply broader services relating to safekeeping and servicing of the crypto-asset, and providers may already be regulated entities. We request that the Commission provide further detail on its definition of a 'wallet provider' and 'custodian', with the view that all firms handling private keys in relation to client assets should fall under this framework.

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

In order to create a level-playing field and to effectively mitigate the risk of ML/TF, all the crypto-asset services in scope of the FATF definition of 'virtual assets' should be consistently captured under the same AML/CFT legal framework obligations. This means that competent authorities should treat relevant crypto-asset service providers on an equal footing in order to mitigate the risk of regulatory arbitrage[18].

Q 43 If a bespoke framework on crypto-assets is needed, do you consider that all crypto-asset service providers covered by this potential framework should become 'obliged entities' under the EU AML/CFT framework? Yes/No/Don't know. Please explain.

In line with our response to Q 42.1, we believe that in order to preserve a level playing field, it is important to ensure that relevant crypto-asset service providers are subject to the same regulation. This can only be achieved if all crypto-asset service providers become 'obliged entities' under the EU AML/CFT frameworks.

This further means that all the entities that provide banking services to VASPs will have to apply a risk-based approach when considering establishing or continuing relationships with VASPs or customers involved in virtual asset activities. This will help to mitigate ML/TF risks emerging from higher-risk virtual assets, virtual asset activities and VASPs.

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?

The industry has developed various technical mechanisms to help mitigate risks arising from peer-to-peer transactions and align with current AML/CFT requirements (e.g., permissioned networks or whitelisting to ensure only on boarded and whitelisted participants are able to hold and transfer assets). It is not yet clear how crypto-assets and their capabilities will continue to evolve. This will need to be taken into account when designing AML/CFT compliance programmes for crypto-assets, and it is important to consider the impact this will have on other relevant legal frameworks.

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/Don't know. Please explain.

AFME believes the FATF standards outlined in Interpretative Note to Recommendation 15 7 (b)[19] should be introduced in the EU AML/CFT legal framework with additional details on their practical implementation. Embedding the FATF standards in the EU framework on crypto-assets will help to achieve a common global taxonomy.

[18] Id. p 9
[19] Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers p56

In line with the FATF Recommendation 10 on preventative measures, documents, data, or information collected under the customer due diligence (CDD) process should be kept up-to-date and relevant by undertaking reviews of existing records[20]. Therefore, holding appropriate information on originators of VASPs, their beneficial owners etc. will allow competent bodies to perform a risk-based analysis on VASPs.

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

- Directors and senior management of such providers should be subject to fit and proper test from a money laundering point of view, meaning that they should not have any convictions or suspicions on money laundering and related offences (5)
- Service providers must be able to demonstrate their ability to have all the controls in place in order to be able to comply with their obligations under the anti-money laundering framework (5)

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

AFME believes that directors and senior management of VASPs should be subject to fit and proper test from a money laundering point of view. The assessment should be done in line with the European Central Bank's (ECB) Guide to fit and proper assessment[21].

Principle 4 from the ECB Guide introduces concepts of proportionality and case-by-case assessment 'the application of the suitability criteria should be commensurate with the size of the entity and the nature, scale and complexity of its activities, as well as the particular role to be filled'[22].

We believe that VASP senior managers should not have any convictions or suspicions on money laundering and related offences. Directors and senior management of VASPs should be the gatekeepers who protect their business against any ML/TF related risks.

However, the fit and proper assessment could only be considered complete when the following information concerning legal proceedings and criminal investigations is carefully considered by the supervised entity and or/prosecution authority:

- The nature of the charge or accusation (including whether the charge is criminal, administrative in nature or involves a breach of trust); the phase of proceedings reached (i.e. investigation, prosecution, sentence, appeal); and the likely penalty if a conviction ensues;
- The time that has passed and the appointee's conduct since the alleged wrongdoing;
- The personal involvement of the appointee particularly with regard to corporate offences;
- Any understanding of and/or insight into his or her conduct gained by the appointee over time; other mitigating or aggravating factors (e.g. other current or past investigations, administrative sanctions imposed, dismissal from employment or any position of trust, etc.); and

[20] Id p27
[21] *Guide to Fit and Proper Assessments*, ECB (May 2018), *available at*: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.fap_guide_201705_rev_201805.en.pdf (hereinafter the "ECB Guide").
[22] Id. p 8

- Assessment of the facts by the appointee and by the supervised entity. The management body should be explicitly asked to examine the pending proceedings and to confirm its confidence in the appointee. This is also important from the perspective of reputation risk for the supervised entity.[23]

3. Consumer/investor protection

Q47 What type of consumer protection measures could be taken as regards crypto-assets? Please rate from 1 (completely irrelevant) to 5 (highly relevant)

- Information provided by the issuer of crypto-assets (the so-called 'white papers') (5)
- Limits on the investable amounts in cryptoassets by EU consumers (4)
- Suitability checks by the crypto-asset service providers (including exchanges, wallet providers, ...) (5)
- Warnings on the risks by the crypto-asset service providers (including exchanges, platforms, custodial wallet providers, ...) (4)

Q 47.1 Any other type of consumer protection measures that could be taken regarding crypto-assets?

Q 47.2 Please explain your reasoning and indicate if those requirements should apply to all types of crypto-assets or only to some of them.

AFME finds that the standards for consumer/investor protection of various categories of crypto-assets should be equivalent to the consumer/investor protection requirements of traditional assets, following the principle of 'same activity, same risk same regulation'. For those crypto-assets that do not map neatly to existing asset classes, there should be minimum standards of consumer/investor protection that leverage existing global principles and guidelines and are tailored to the risks that these new types of crypto-assets entail.

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. Please explain.

AFME finds that the standards for consumer/investor protection of various categories of crypto-assets should be equivalent to the consumer/investor protection requirements of traditional assets, following the principle of 'same activity, same risk same regulation'. For those crypto-assets that do not map neatly to existing asset classes, there should be minimum standards of consumer/investor protection that leverage existing global principles and guidelines and are tailored to the risks that these new types of crypto-assets entail.

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. Please explain.

As is the same for traditional asset classes, following the principle of 'same activity, same risk same regulation', the level of consumer/investor protection should be commensurate to the sophistication and risk appetite of the user (i.e. different protection levels may be required for each client category). Therefore, if in a private sale the identified parties are qualified or institutional investors, the standard of consumer/investor protection should be equivalent to that of traditional investments. Similarly, the standards of protection for retail facing issuance will need to be appropriately tailored.

[23] Id. p 13/14

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.

AFME finds that the standards for consumer/investor protection of various categories of crypto-assets should be equivalent to the consumer/investor protection requirements of traditional assets, following the principle of 'same activity, same risk same regulation'. For those crypto-assets that do not map neatly to existing asset classes, there should be minimum standards of consumer/investor protection that leverage existing global principles and guidelines and are tailored to the risks that these new types of crypto-assets entail.

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

As with any other traditional asset, crypto-assets require global coordination. This could include requiring providers to abide by some minimum standards in order to be able to offer their services in the EU in order to avoid unfair competition, regulatory arbitrage and offer some minimum level of consumer/investor protection. For more detail see our response to Q 48.

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 supervision by the European Authorities (in cooperation with the ESCB where relevant)?

AFME has not responded to this question.

Q 53 What tools would EU regulators need to adequately supervise service providers and their underlying technologies?

AFME finds that the standards for consumer/investor protection of various categories of crypto-assets should be equivalent to the consumer/investor protection requirements of traditional assets, following the principle of 'same activity, same risk same regulation'. For those crypto-assets that do not map neatly to existing asset classes, there should be minimum standards of consumer/investor protection that are based upon existing global principles and guidelines.

With this in mind, we believe crypto-asset service providers would need to be brought into the scope of EU regulators by virtue of becoming regulated entities in a risk-based and proportionate manner, in order to mitigate the above mentioned risks to consumers/investors, and also market and financial stability risks (see our response to Q 11, 13). Transparency and governance provisions would be important in order to supervise such entities and their underlying technologies.

It might be that in order to futureproof the oversight of regulated activities that are conducted using DLT, EU regulators could look to obtain a real-time transparency of the actions taking place on the network. This could be made possible through the addition of real-time regulatory supervisory 'nodes' in DLT ecosystems[24]. We encourage the industry and regulators to collaborate in trailing the use of real time supervisory nodes and other components of the technology in experiments and proof of concepts in those areas where they could add value in order to benefits to both public and private sectors.

[24] *See* Raphael Auer, *Embedded Supervision: How to Build Regulation into Blockchain Finance*, BIS Working Papers No 811, BIS (Sep. 2019), *available at*: https://www.bis.org/publ/work811.pdf.

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

A. General questions on 'security tokens'

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

AFME has not responded to this question.

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 – completely disagree)

55.1 please indicate specific areas where the tech could provide the most efficiencies compared to the legacy system

AFME completely agrees that DLT could be used to introduce efficiencies or other benefits, particularly in the areas of post trade, custody and settlement. However, we also note that there are a number of potential risks and issues which could emerge from the introduction of DLT into those activities, and these would need to be mitigated, particularly by the application of effective regulations. For more detail see our response to Q10.

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 neutral agree/disagree). Please explain.

There is a path of evolution and adoption that applies to any new technology, which includes testing and evaluation of appropriateness for any intended use. Some of those considerations include standards, performance, scalability, cybersecurity and interoperability.

As with all digitisation or technological innovation in financial markets, new risks can emerge when they develop ahead of the regulatory or legal framework. Therefore, it is important that any regulatory framework that is introduced is sufficiently flexible and dynamic to account for the rapid development of technology in this space.

The industry stands ready to work with policymakers to ensure that best practices are applied with respect to the creation or use of new technologies that support traditional financial activity. Regulators and market participants will need to continue to assess any possible additional risks, such as cyber and operational risks, and reflect that analysis in the risk assessments of assets and activity surrounding the assets.

Q 57 Do you think DLT will significantly impact the role and operation of trading venues and post trade FMIs (CCPs, CSDs) in the future (5-10 years time)? Please explain.

This will depend on the evolution of the technology and the uses that market participants explore with that technology, as well as the possibility and feasibility of safe interoperability. It will also depend on the evolution of the regulatory framework, as the role of Central Security Depositaries (CSDs), Central Counterparties (CCPs) and Trading Venues are inherently defined in regulations such as the Central Securities Depositories Regulation (CSDR), European Market Infrastructure Regulation (EMIR), and MiFID.

To the largest extent possible, the rules that apply to Financial Market Infrastructures (FMIs) in the current environment should equally apply to any DLT platforms performing similar roles. This is not only to ensure a level playing field, but

more importantly because the current regulations and regulated FMIs have been put in place to ensure the safety and stability of the market and reduce systemic risk.

The role of FMIs will remain important, but the operation of the platforms may evolve as a result of the use of DLT and other technology. For example, many of the efficiencies that may be gained in clearing, settlement, custody, and other activities may streamline some of the now manual processes market participants perform. This streamlining may lead to commoditization and automation of various businesses and processes, while at the same time may create new opportunities for market participants.

As the applicable regulations like MiFID, EMIR, CSDR, and others have been written with the current operational and technical set-ups in mind, it is possible that a number of provisions no longer apply or do not apply in the same way for DLT driven processing. For example, reconciliation of positions and movements may occur in a different way on a DLT platform. Finality of settlement can also be achieved in a new way; there could be less reliance on offline data transmission and processing and an increase in business processes being applied directly to data on a shared DLT. Some of these changes may require regulators to re-evaluate the appropriateness of existing regulation.

Therefore, any change in the role of a CSD, CCP or Trading Venue, or evolution in the activities they perform would need to be considered by regulators as part of their review of current regulations.

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

AFME believes the safety and soundness of the system should prevail, and that core infrastructures should be regulated.

However, we recommend remaining technology agnostic and risk-based while providing guidance and clarity on how DLT can be leveraged in financial transactions, rather than on specifics on a network or technology (e.g. permissioned versus permissionless networks). This is an important principle to future proofing the EU regulatory framework, encouraging innovation and fostering a level playing field.

While AFME acknowledges the design of the network will impact current feasibility in alignment with regulatory frameworks and guidance, this technology continues to evolve, and solutions may rapidly arise to allow a variant of the technology to be used in alignment with regulatory requirements. For example, generally, alignment with KYC/CFT requirements maybe possible in both permissioned (e.g., a closed of network with known market participants) and permissionless networks (e.g., through whitelisting and transfer restrictions). However, AFME supports that implementation and alignment with KYC / CFT requirements may be more scalable in permissioned networks. AFME also notes that both permissioned and permissionless DLT networks have been leveraged to facilitate financial activity [25] [26] [27].

As the technology matures AFME supports collaboration with the Commission through sandboxes and innovation forums, such as the European Forum for Innovation Facilitators (EFIF). This will enable regulators to facilitate the

[25] *Santander Launches the First End-to-end Blockchain Bond*, Santander (Sep. 12, 2019), *available at*: https://www.santander.com/en/press-room/press-releases/santander-launches-the-first-end-to-end-blockchain-bond%C2%A0

[26] *CBA Chosen By World Bank to Deliver World's First Blockchain Bond,* CommBank (Aug. 10, 2018), *available at*: https://www.commbank.com.au/guidance/newsroom/cba-picked-by-world-bank-to-deliver-world-s-first-standalone-blo0-201808.html

[27] *Societe Generale Issued the First Covered Bond as a Security Token on a Public Blockchain,* Societe Generale (Apr. 23, 2019), *available at*: https://www.societegenerale.com/en/newsroom/first-covered-bond-as-a-security-token-on-a-public-blockchain

development of this technology in a safe environment that protects investors and market integrity, whilst enabling regulators to continue to consider how to regulate financial services activity using different solutions, ensuring the provision of sufficient legal certainty, finality, and consumer/investor protection.

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 – disagree). Please explain.

We find that the absence of a common approach on when a security token constitutes a MiFID "financial instrument" discourages innovation and investment in technology and products. It also increases compliance risks and costs. This is particularly the case for market participants operating in multiple jurisdictions and cross-border both in the EU and globally.

Q60 If you consider that the absence of a common approach on when a security token constitutes a financial instrument is an impediment, what would be the best remedies according to you? (1 not relevant – 5 very relevant)

- **Harmonise the definition of certain types of financial instruments in the EU (5)**

  An integrated securities market requires consistent definitions of fundamental legal and operational concepts. Without consistent definitions, investors and other market participants are faced with significant complexity and risk in their market activities. However, changes to the definition of a financial instrument should not affect the substance of the application of the regulatory regime to 'traditional' financial instruments.

- **Provide a definition of a security token at EU level (1)**

  AFME does not recommend creating a new category of "financial instrument" under MiFID II itself in order to accommodate security tokens as this may risk changing the regulatory perimeter. This is not considered necessary or desirable as a policy approach (instruments which have the characteristics of an existing category of "financial instrument" regardless of the underlying technology should be subject to the same regulatory perimeter as 'traditional' instruments), and could have unintended consequences. On the other hand, a sub-asset class definition (within the existing MiFID categories of "financial instrument") might be a useful categorisation device if it is decided that the application of MiFID conduct of business or other rules (i.e. other than the authorisation perimeter) should be applied differently to DLT based instruments (see our response to Q 71, 72, 74 and 76 below).

- **Provide guidance at EU level on the main criteria that should be taken into consideration while qualifying a crypto-asset as a security token (5)**

  Clear and practical guidance would help to ascertain (more consistently across member states) whether a security token will constitute a financial instrument, including the particular category of financial instrument (it is noted that the definition of "transferable securities" can be particularly difficult to apply, and clarification on what is considered negotiable in a DLT context might also be helpful). Provided that it was drafted in a sufficiently non-prescriptive way, the guidance would go some way in preventing regulatory arbitrage. The guidance should align as closely as possible to the criteria of traditional MiFID financial instruments.

Whilst the guidance should be technology neutral, it needs to address those technological aspects of security tokens which cause difficulties in determining whether a security token constitutes a financial instrument. In doing so, it could set out indicative situations, circumstances and characteristics. An approach that focusses on the function of the security token is preferred (as opposed to, for example, an approach that focusses purely on labelling and characteristics).

Within the guidance it could be helpful to indicate the sub-asset classes of "security token" to which the guidance applies, if (covered by later questions) there are subsets of MiFID II rules that need to be exempted or varied for DLT based instruments. Any guidance will need to consider the following points:

- Whether native security tokens should be considered fungible with tokenised securities (i.e. those tokens representing interests in underlying financial instruments).
- Whether security tokens are fungible with traditional financial instruments in the same sub-asset class.

It is worth noting that the structure of MIFID II already accommodates application of certain rules to certain instruments to fine tune the application of the rule set. For example, MIFID II does not include structured deposits in its list of MIFID II financial instruments but they are subject to the investor protection rules. (See also our response to Q 63 below).

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

AFME has not responded to this question.

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)? (1 – 5 very relevant factor)

- In answering this question we consider two example (non-exhaustive) forms of hybrid crypto-assets:
  - Tokens with multiple functions/characteristics at issuance
  - Tokens which change and take on additional functions/characteristics during lifecycle

- **Hybrid tokens should qualify as financial instruments/security tokens (3)**

  Yes. Crypto-assets that contain the characteristics of a financial instrument should be treated as such. Hybrid tokens with multiple characteristics at issuance that meet the definition of a financial instrument at the outset should be categorised as such at that point in time. Hybrid tokens with multiple characteristics over time present additional challenges, and we request further clarification from the Commission on how these will be classified (some considerations are provided in the paragraph below). We note that careful consideration should be given as to where a crypto-asset is potentially covered by one or more regulatory frameworks, as all respective obligations will need to be satisfied. Please see our response to Q 8 for more detail on our views on hybrid tokens.

- **Hybrid tokens should qualify as unregulated crypto-assets (i.e. like those considered in section III. of the public consultation document) (3)**

  Only insofar as hybrid tokens do not constitute MiFID financial instruments, which may only be for a limited portion of the lifecycle of a hybrid token. For crypto-assets that have conditional conversion events built into the terms at issuance, any change in the regulatory treatment of the token should be on the occurrence of the relevant conditional event. As noted above, the additional functions/characteristics of a crypto-asset should not prevent a crypto-asset that meets the definition of a financial instrument from being treated as such although the regulatory obligations applying to that crypto-asset should be carefully considered.

- **The assessment should be done on a case by-case basis (with guidance at EU level) (5)**

Yes. Not just on a per instrument point in time basis, but per instrument subject to ongoing review throughout the lifecycle of the instrument. Regulators should provide appropriate and clearly defined rules and/or guidance on how to assess when regulatory treatment would change. Should new types of hybrid tokens develop over time, their treatment should be considered as they develop.

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

AFME has not responded to this question.

Q62 Do you agree that the existing rules and requirements for investment firms can be applied in a DLT environment? (Completely agree, rather agree, neutral, rather disagree, completely disagree). Please explain.

We rather agree, as there are some unique considerations around leveraging DLT that may not exist today, which will require additional guidance from regulators in order to encourage the development of innovative and efficient technological models, whilst still protecting investors and intermediaries.

Whatever network configuration and consensus protocol is used by an issuing entity will need to ensure that the entity can carry out the functions it is authorised to perform. Based on the current technology, aligning with regulation may vary in difficulty depending on the design of the DLT network. For example, with a fully decentralised DLT network it may be difficult to assign a trusted intermediary to confirm transactions, given the decentralised way the network confirms transactions and stores or adds new data. Currently we are of the view that additional investigation would be required in order to determine the best way to regulate security tokens falling within the scope of MiFID which exist on a permissionless network.

In general, it seems that the existing rules and requirements for investment firms can at this point be more easily applied within a permissioned DLT environment, subject to certain clarification, amendment and potentially disapplication in relation to some specific obligations (e.g. see our response to Q 71 below). AFME would suggest that, given the challenges with applying the existing MiFID rules, particularly to permissionless networks, that regulators focus their initial efforts in calibrating the MiFID framework to apply to security tokens on permissioned networks.

However, the market continues to develop and test technology related to DLT, to align with current requirements. For instance, there may be opportunities to program various controls that can fulfil regulatory obligations, which the industry is currently exploring today. As crypto-assets continue to evolve and the underlying technology matures, it is important that regulation remains technology neutral to allow for the development of these technologies that may provide benefits in the future.

Q63 Do you think that a clarification or a guidance on applicability of such rules and requirements would be appropriate for the market? Please explain. (Completely agree – completely disagree)

While we believe the rules and principles embodied in MiFID are appropriate for security tokens, as they were not originally designed with crypto-assets or DLT in mind, therefore guidance or clarification is needed to ensure the existing framework is fit for purpose to ensure the full functionalities of crypto-assets can be utilised appropriately.

A non-exhaustive list of areas where clarification might be needed include:

- **Transparency calculations –** Clarification is needed in relation to liquidity classification of financial instruments, sizes large in scale compared to normal market size (LIS) and size specific to the instrument (SSTI)

in the context of security tokens categorised as non-equity financial instruments, and liquidity classification and tick size band assessment in the context of security tokens categorised as equities.

- **Tokenisation of an existing financial instrument -** Clarification is needed on whether tokenisation of an existing financial instrument creates a new, additional financial instrument, and whether they are fungible.
    - We are of the view that where a token is a digital representation of an already existing financial instrument (i.e. the issuer is the same, all the characteristics are the same (including economic and legal rights and obligations), then the token is not a new financial instrument, but another means of reflecting holdings in such instruments. In essence, the DLT plays a role of books and records not dissimilar to e.g. the current books and records of custodians and agent banks, which do not alter the nature of the financial instrument or the entitlements attached to it.
    - Where the token is a representation of a financial instrument that has different characteristics from the underlying instrument, e.g. the issuer is different, or the rights, entitlements and obligations associated with the token are different from the ones associated with the underlying financial instrument, for example in the case of an ADR, then our assumption is that they should be treated as a new instrument separate from the underlying financial instrument. If the characteristics of that token are similar to the ones commonly associated with financial instruments, then they should also be classified as financial instruments and be treated accordingly under the same rules.
- **Transactions that move on and off-chain (DLT) –** Clarification is needed on how these should be treated.
- **Application of the algorithmic trading and high-frequency trading (HFT) rules.**
- **DLT networks with nodes in multiple jurisdictions –** Guidance is potentially needed in relation to conflict of laws issues raised by the nature of the network structure.

Q64 Do you think that the current scope of investment services and activities under MiFID II is appropriate for security tokens? Please explain. (Completely agree – completely disagree)

AFME considers that the current list of investment services and activities under MiFID II can and should apply equally to security tokens that constitute financial instruments.

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.

AFME has not responded to this question.

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.

There are various efforts related to leveraging DLT to perform trading venue functions. Below are some points of discussion:

Legal issues:

Clarification is necessary on:

- What constitutes a trading venue in a DLT environment;
- The status of a node in a DLT environment (please see our response to Q 19 for more detail);
- Execution requirements specific to a DLT environment – including whether/when execution is considered to take place on the DLT itself, particularly in those cases where there is off chain matching later recorded on-chain;
- Access to trading venues and how that will be impacted by on chain/off chain execution/settlement;
- The application (or not) of non-discriminatory access rules (CCPs and trading venues) and clearing requirements to DLT;
- How matched principal/AOTC trading may occur in a DLT network; and
- How price formation may occur in a DLT network.

Operational issues:

- There is a question as to whether the mechanism for recording ownership and changes in ownership is consistent with the prohibition on Multilateral Trading Facilities (MTFs) and in some cases, Organised Trading Facilities (OTFs), from taking proprietary positions.

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/No/ Don't know no opinion.

Traditional financial instruments and security tokens should be subject to the same investor protection rules; the use of a particular technology does not change the nature of the asset. Any clarifications provided in relation to the application of investor protection rules to security tokens that constitute financial instruments should be mapped against existing requirements. Clarification could for example be provided on the following areas:

- **Appropriateness** - how the distinction between complex and non-complex products applies in respect of security tokens;
- **Client identification** – For suitability/appropriateness assessments (we note that the scope of the rules is appropriate but that clarification will be needed on the specific application to security tokens)
- **Disclosure to clients** –
    - Information to be provided on safeguarding client assets (see also our response to Q 63 above);
    - Risk disclosures applicable specifically to the additional risk features of security tokens;
    - Costs and charges information;
- **Product governance** –
    - The application of the product governance obligations, in particular who the "manufacturer" and "distributor" are in the security token/DLT model; and
    - Identification of target markets.

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.

We consider that traditional financial instruments and security tokens should be subject to the same marketing requirements.

Q69 Would you see any particular issue (legal, operational,) in applying MiFID investor protection requirements to security tokens? Please explain your reasoning.

Please see our response to Q 63.

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.

AFME has not responded to this question.

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

There are various efforts related to leveraging DLT to perform trading venue functions. For the purposes of this question, it is assumed that execution or order matching occurs on DLT. However, it can also happen off-chain and in a traditional order book, which is later recorded on a DLT networks in batches, due to timing issues. Please see our response to Q 66 above highlighting the need for clarification on this point.

Electronic trading in a DLT environment could potentially be sufficiently different to require additional rules or guidance., as some of the detail of the current rules would not workably translate to a DLT environment. The current regulatory framework was not originally designed with crypto-assets or DLT in mind, as it is based primarily around bilateral relationships rather than the multilateral nature of distributed financial networks. Clear and practical guidance would help to ascertain (more consistently across member states) whether a DLT can facilitate requirements of electronic trading, provided that it was drafted in a sufficiently non-prescriptive way.

Clarification may be required on, to name a few:

- Sufficient "capacity" in a DLT environment;
- BCP requirements in a DLT environment; and
- How cancellation/kill switch requirements apply in a DLT environment.

DEA is addressed under our response to Q 73 below.

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

It is assumed that the Prospectus Regulation will apply to security tokens that qualify under that legislation. See also our response to Q 82 to 87.

Legal issues:

- There could be challenges in applying these requirements on a fully decentralised network with no legal operator, particularly if it were possible to make a token "available to trade" in a similar way that e.g. bonds can be made available to trade without the consent of the issuer.
- Fungibility will be key to the details of how the admission/suspension/removal rules will work in practice:
- In line with current practice in relation to traditional instruments, the suitability of the following approach should be considered:
    - Any tokens fungible with a traditional financial instrument should also be suspended/removed and vice versa;
    - Any derivatives/tokens representing linked derivatives should also be suspended/removed; and

- Tokenised securities should be suspended/removed if the related traditional asset is suspended or removed.

Operational issues:

- The admission to trading of security tokens that are financial instruments. Some of these relate to technological assurances and testing;
- The issuing developers behind the security token;
- The type and details of the DLT used;
- Hacking vulnerabilities and traceability of the security tokens.

In the absence of accepted industry standards, it will be difficult to assess whether from an operational perspective an instrument should be admitted to trading.

Q73 What are the risks and benefits of allowing direct access to trading venues to a broader base of clients? Please explain your reasoning.

AFME has not responded to this question.

Q74 Do you think these pre- and post-transparency requirements are appropriate for security tokens? (Completely agree, neutral rather disagree, completely disagree). Please explain.

While transparency principles set out in EU regulation should apply to security tokens as well as traditional financial instruments, the actual implementation of the principles could require some regulatory guidance to accommodate for the way transparency is achieved. Given the potential changes in requirements that are currently ongoing, we recommend that pre-trade transparency and post-trade transparency requirements should be subject to further consultation separately at a later date.

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.

Please see our response to Q 74.

Q76 Would you see any particular issue (legal, operational) in applying these requirements [transaction reporting and obligations to maintain records] to security tokens which should be addressed? Please explain your reasoning.

Yes, we note that clarification may be needed to ensure the appropriate controls are in place. We note some examples including:

- International Securities Identification Numbers (ISINs) and the extent to which these are available in relation to security tokens – query whether a security token would have the same ISIN as its underlying security (where the security token itself does not constitute the share);
- Reporting fields/requirements may need to be revised to appropriately report security tokens in case different fields needed than in the case of traditional instruments; and
- Whether a security token is fungible with its non-digital counterpart.

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.

Yes, while we consider that the current scope of Article 8 of the Market Abuse Regulation (MAR) on insider dealing is appropriate to cover all cases of insider dealing for security tokens, Article 8 of MAR will only apply to security tokens to the extent they are deemed to be in-scope under Article 2 of MAR (i.e. financial instruments which are admitted to trading on a regulated market (or where a request for admission has been made, as applicable, or traded on MTFs or OTFs), or where the price or value of that instrument depends on or has an effect on the price or value of an in-scope financial instrument). As a result, Article 8 of MAR will only be fit for purpose where clarification is provided on what constitutes a trading venue in a DLT environment. If the current definition of "trading venue" remains un-amended, it is likely that the trading of security tokens may fall outside of the provisions of Article 8 of MAR, unless they reference financial instruments which are themselves in-scope of MAR.

In addition, if there are new innovative unregulated crypto-assets, whose values are directly or indirectly referenced to regulated financial instruments, then it would be possible for insider dealing to be committed using unregulated crypto-assets. Therefore, the scope of MAR and MiFID should be continually reviewed to assess the need for new, unregulated crypto-assets to be captured. In many ways, this mirrors the recognised necessity of bringing over the counter financial derivatives that reference shares, bonds or other securities within the scope of MAR.

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.

For security tokens that are tradeable on an electronic platform in all cases, the notion of market manipulation as defined in Article 12 of MAR would apply, however there may also be new instances of market manipulation that should be considered.

In order to assess whether the notion of market manipulation, as defined in Article 12 of MAR, is sufficiently wide to cover instances of market manipulation of security tokens, it would be helpful to first clarify how trading in security tokens which constitute financial instruments may be conducted. This would include whether this is conducted (i) on a trading venue (what constitutes a trading venue in a DLT environment itself to be clarified) or (ii) not on a trading venue, where security tokens themselves reference in-scope financial instruments. It is conceivable here that novel types of market manipulation could arise.

Regarding the detection of market manipulation, including in particular where security tokens reference in-scope financial instruments but are not traded on a trading venue, the tools available for and sources supporting the detection and prevention should be considered (e.g. reporting, transparency, supervision, market surveillance systems and activities).

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?

Yes, for derivatives (i.e. financial instrument security tokens) whose value is based on an underlying crypto-asset. In addition, see responses to Q 77 - 78.

Q 80 Have you detected any issues that would prevent effectively applying SSR to security tokens? Please rate from 1 (not a concern) to 5 (strong concern). Please explain.

- Transparency for significant net short positions (4)
- Restrictions on uncovered short selling (4)
- Competent authorities' power to apply temporary restrictions to short selling (4)

80.1 Any other issues that would prevent effectively applying SSR to security tokens?

AFME supports the European Securities and Markets Authority's (ESMA) advice to the Commission[28] where it notes that a security token could be captured by the Short Selling Regulation (SSR) if it confers a financial advantage in the event of a decrease in the price or value of a share or sovereign debt.

We agree that the list of instruments in Annex I of Delegated Regulation 918/2012 needs expanding in scope (e.g. does not currently include a transferrable security).

However, we note that any changes to the SSR should also ensure that the exemption for market making activities contained in Art. 17 of the SSR is appropriately expanded/amended to enable market makers in security tokens to take advantage of the exemption where appropriate. As per Recital 26 of the SSR, 'market making activities play a crucial role in providing liquidity to markets within the Union and market makers need to take short positions to perform that role'. Accordingly, it should be acknowledged that if security tokens are deemed to be instruments which give rise to a position in shares or sovereign debt, the market making exemption in the Level 1 text and the ESMA Guidelines on Market Making[29] should be appropriately calibrated to be used where firms carry out market making activity in security tokens. This review should include a consideration on whether the trading venue membership aspect of the definition in Art. 2(1)(k) of the Level 1 text is fit for purpose (noting that security tokens may not necessarily be traded on 'trading venues'). It should also ensure that the ESMA Guidelines acknowledge that positions in, or hedges of, security tokens are eligible for the exemption.

Our understanding of DLT today is that it is difficult to short sell crypto-assets without a conventional contractual agreement similar to that for repo or stock borrowing/lending. Nevertheless, it should be possible to define the value of an unregulated crypto-asset to be based on the value of a short position in conventional shares or bonds. In that case, holding a long position in such a crypto-asset would be equivalent to holding a short position in a share or bond.

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.

AFME has not responded to this question.

4. Prospectus Regulation (PR)

AFME Introductory remarks

AFME recognises the important role that the prospectus plays in providing a description of a company's business, its finances, its shareholding structure and the securities that are being offered and/or admitted to trading. AFME also recognises that the prospectus contains important information investors need before deciding whether to invest in a company's securities.

[28] *Initial Coin Offerings and Crypto-assets,* ESMA (Jan. 9, 2019), *available at*: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

[29] Exemption for market making activities and primary market operations under Regulation (EU) 236/2012 of the European Parliament and the Council on short selling and certain aspects of Credit Default Swaps, ESMA (March 2013) *available at*: https://www.esma.europa.eu/sites/default/files/library/2015/11/2013-74.pdf

We believe that regulation should be product and technology agnostic. In AFME's view, if a tokenized product embodies the features of a conventional security (e.g. a bond or a share), then it should be regulated in the same manner as that conventional security.

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

AFME does not believe that different or additional exemptions (other than the ones laid down in Article 1(4) and Article 1(5) of the PR) should apply to security tokens. If a security token is designed to perform the function of a conventional security, then it should be subject to the same requirements under the Prospectus Regulation as that conventional security.

Allowing security tokens to benefit from additional exemptions under the Prospectus Regulation presents the risk of regulatory arbitrage and could result in investors in such instruments losing access to important information about the security token and its issuer (including information relating to risk factors) that would be included in a prospectus for conventional securities. We believe that it is important for investors to be able to access such information, particularly if a security token presents any inherent underlying risks related to the methods of transferring and holding securities structured in this way (e.g. in relation to DLT).

AFME would welcome an opportunity to engage with the Commission to understand better the rationale behind this question.

Q 83 Do you agree that Delegated Regulation (EU) 2019/980 should include specific schedules about security tokens? Yes/No/Don't know

Q83.1 Please explain your answer to question 83.

AFME believes that the concept that underpins Article 6 of the Prospectus Regulation, which requires the prospectus to contain the necessary information which is material to an investor for making an informed investment decision, applies equally to security tokens as it does to other types of securities. This means that the Prospectus Regulation regime already requires disclosure of material risks and the key features that are specific to the securities being offered or admitted to trading.

We consider there is no perceived need for Delegated Regulation (EU) 2019/980 to include specific disclosure requirements about security tokens at this point. However, if, as the market for security tokens develops, varied interpretations arise as to how the overarching Article 6 disclosure test or specific existing annex disclosure requirements are met in the security tokens space, depending on the approving National Competent Authority (NCA), this position may change. This would be contrary to the principles of a European common market and could result in uncertainty regarding whether a prospectus that has been approved in an EU Member State can be passported into other Member States.

As market practice develops there should be more clarity around the risks specific to DLT as well as how such risks should be presented in prospectuses. Depending on how the market for security tokens develops, it might be helpful for ESMA, at an appropriate time, to provide Level 3 guidance in the form of a Q&A in order to facilitate market consistency.

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

AFME has not responded to this question.

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

As detailed in our response to Q 82, we believe that a security token that performs the function of a conventional security should be subject to the same requirements under the Prospectus Regulation as that conventional security. We also think that, at this time, it is premature to assess whether any of the types of prospectuses listed in Q 85 should be amended for security tokens, as very few prospectuses for security tokens have been issued in the European markets.

Q 86 Do you believe that an ad hoc alleviated prospectus type or regime (taking as example the approach used for the EU Growth prospectus or for the simplified regime for secondary issuances) should be introduced for security tokens? Yes/No/Don't know.

As set out in our responses to Q 82 and 85, we believe that a security token that performs the function of a security should be subjected to the same requirements under the Prospectus Regulation as that conventional security. AFME's view is that, from an investor's perspective, a security token presents the same risks as does a conventional security and could present additional risks relating to the token's underlying technology. Separately, existing alleviated prospectus disclosure regimes, such as the EU Growth prospectus, might be available to issuers of security tokens. Therefore, we do not believe that an ad hoc alleviated prospectus type or regime should be introduced for security tokens.

Q 87 Do you agree that issuers of security tokens should disclose specific risk factors relating to the use of DLT? (Completely agree – completely disagree)

While AFME believes that issuers of security tokens should disclose specific risk factors relating to the use of DLT, we do not think that ESMA's guidelines on risk factors need to be amended to cater for security tokens. As set out in our response to Q 83, Article 6 of the Prospectus Regulation already requires the prospectus to contain necessary information which is material to an investor for making an informed investment decision, including, we assume, material risks related to DLT, and the key features that are specific to the securities being offered or admitted to trading.

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

- Definition of 'central securities depository' and whether platforms can be authorised as a CSD operating a securities settlement system which is designated under the SFD (3)
- Definition of 'securities settlement system' and whether a DLT platform can be qualified as a securities settlement system under the SFD (3)
- Whether records on a DLT platform can be qualified as securities accounts and what can be qualified as credits and debits to such an account (3)
- Definition of 'book-entry form' and 'dematerialised form' (2)
- 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) (2)

- What could constitute delivery versus payment in a DLT network, considering that the cash leg is not processed in the network (3)
- What entity could qualify as a settlement internaliser (2)
- Other

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

The current legal and regulatory framework set out in CSDR is robust and well-founded, and provides the correct level of protection, control and governance. Current risks associated with post-trade settlement are appropriately mitigated. There should not be a dilution of the regulatory obligations under CSDR when extended to a DLT environment. These obligations should continue to apply in respect of all in-scope securities, including issuance of such securities on a DLT platform. This requires clarification of the obligations of a CSD under CSDR to account for the adoption of DLT and possible variations in the methods of legal ownership of interests in securities. We encourage the Commission to consider reviewing CSDR to cater for the nascent nature of DLT.

In the context of security tokens, we consider DLT can provide the same functionality as current technology used by traditional CSDs. AFME's preferred approach would be to retain the role of a CSD, with a guiding principle of 'same activity, same risk, same regulation', to ensure that the regulatory landscape remains technologically neutral.

Role of a traditional CSD

The industry values the robust regulation of CSDs, as a critical market infrastructure and centralised point of control for the issuances of traded/ listed securities. The key roles of a CSD are:

- Recording of securities in book-entry form at the outset;
- Reconciliation of the amount issued with holdings of CSD participants;
- Control of changes in legal ownership of the securities; and providing settlement finality.

These elements are still capable of being met mutatis mutandis by a CSD operating in a DLT environment, provided adjustments and clarifications are made. We explore this further below.

CSD operating in a DLT environment

Regarding security tokens, the distributed ledger typically represents the dematerialised form of the security by directly recording the ownership rights of wallet holders, i.e. the distributed ledger is the definitive and correct record of legal ownership, similar to the records of traditional CSDs. The CSD ensures that the amount of security tokens issued is always equal to the sum of the tokens held by wallet holders. Transfer of ownership in a security token is represented by updates to the distributed ledger. Settlement occurs upon validation of the transaction and the resulting update to the ledger. This assumes that there is a precise definition and application of settlement finality (see our response to Q 93).

The specific role of the CSD in the context of DLT securities settlement must be assessed against similar functions under the traditional environment. Where these functions and terms are described differently (e.g. wallet vs security account), harmonisation is required. In a DLT environment, legal title no longer resides solely on the books of a CSD. Rather, it is assumed that the CSD may play a new role of operating the DLT network, recording, controlling and facilitating the transfer of legal title of securities, by overseeing the DLT-based system and having validation rights e.g. via a master key.

The robustness of this technical control must be proven on a case-by-case basis, given the variety of technical means by which one can establish DLT network entitlements, and the different technical protocols and implementation of consensus mechanisms. Notwithstanding this, there should be no dilution of the obligations of CSDR.

Additional practical roles that could be performed by a central authority, such as a CSD, could involve the following, although these may be outsourced or performed by another entity:

- Access control and connectivity;
- Identity checks;
- Maintenance of cash accounts and/or cash tokens and processing of cash transactions;
- Provision and maintenance of DLT infrastructure and protocols; and
- Coding and management of smart contracts.

While many of the roles above are similar to those performed by CSDs today, there is no legal certainty as to whether these new roles would fall within the existing definitions of CSDR 'core' or 'ancillary' services', we would welcome such clarity.

Requirements under CSDR

CSDR aims to harmonise aspects of the settlement process and provide a common set of requirements applicable to CSDs. CSDR requirements can be categorised into three main themes:

1) Authorisation and requirements applicable to CSDs;
2) Settlement discipline; and
3) Internalised settlement.

These obligations are robust and well-founded, though we welcome guidance on how a CSD operating in a DLT context would comply with certain requirements that are not currently technologically neutral. Clarification is helpful to eliminate barriers to entry, as discussed in our response to Q 91. Importantly, none of our observations are intended to suggest a dilution or variation of CSDR and its intended outcomes. CSDs operating in a DLT environment should be required to comply with the same or equivalent standards of CSDR.

Q 88.2 Please explain your reasoning for your answer to question 88.

i. *Definition of a central securities depository*

Broadly, the current definition of a CSD is appropriate for DLT based securities. However, we have some concern with:

- **The concept of 'initial recording of securities'** - an issuer seeking to issue securities tokens on a DLT network would need to appoint a CSD for the issuance. That CSD will, in combination with the issuer, police the establishment and control of the DLT-based register. The issuer's act of dematerialisation is the placing of securities on the DLT-based register. Provided the CSD agrees to carry out its establishment and control functions, it seems that the CSD's role would broadly equate to the initial recording of securities in a book-entry system. Clearly, the language of CSDR does not cater for DLT issuance, however, it is not outside the conceptual meaning of this provision. Whilst AFME does not see this as an inherent challenge, further clarity would be helpful in the form of regulatory guidance or amendments to CSDR.

- **The concept of 'top tier level' maintenance** - It is essential that there is a control function performed by a responsible entity to ensure that the 'top tier' level holdings reflected in the securities accounts ("wallets") are

correct. The process may vary depending on the network and protocol and may require the ability for a CSD to have a master node or similar control.

- **The use of 'central' in the definition** - we welcome clarification that a central view of accounts can be maintained by a decentralised database, e.g. a CSD could make use of DLT infrastructure.

ii. 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?

While CSDR defines a securities account it does not explicitly state whether there is a legal difference between accounts, records and ledgers. Our assumption is that the notion of 'wallets' is similar to that of accounts. Clarity is welcomed.

In a DLT context, we assume that a CSD should, through technological means, be able to control any attempts to transfer title; and to record and clearly reflect at any point current ownership. AFME's view is that there is significant value in a single entity performing this role.

iii. Definition of 'book-entry form' and 'dematerialised form'

We see no inherent challenge with these definitions although AFME's view is that the concept of book-entry form ought to be clarified/broadened to include entries on a DLT ledger.

iv. What could constitute delivery versus payment in a DLT network, considering that the cash leg is not processed in the network?

The most significant source of credit risk in securities settlement, and, therefore, the most likely source of systemic risk is the principal risk that may arise on the settlement date. Such principal risk can be eliminated if the securities settlement system adheres to the principle of, as required by Article 39.7 of CSDR. Delivery versus Payment (DvP) is achieved today in systems such as TARGET2-Securities (T2S), where the Eurosystem operates the cash and securities entries on behalf of all parties in Central Bank money, or it can be done by a licensed commercial bank, which operates cash accounts in commercial bank money.

In the context of a DLT-based security token settlement, technical/operational solutions might be utilised to achieve DvP, or something similar. We note research by the Bank of Japan and European Central Bank into how to technologically achieve DvP in a DLT environment[30]. On the assumption that the technical/ operational solutions are workable, we welcome clarification on the possibility from a legal perspective.

Clarification is required on what the exact set-up and applicable DVP model is, who the provider of cash services is, what the interface model is, and what the credit and collateral management services are. The applicable provisions of CSDR, and regulatory technical standards on prudential requirements for CSDs and designated credit institutions offering banking-type ancillary services should also apply to such set-ups and institutions.

v. Definition of settlement internaliser

A settlement internaliser is an entity (acting as a custodian for both parties to a trade) that receives a settlement instruction from a client but does not forward it on to another entity in the securities holding chain. Instead, the settlement instruction results in a transfer of securities from one account to another across the books of the settlement internaliser itself without the movement taking place on an external securities settlement system of the CSD. On the

[30] Joint bank of Japan and European Central Bank Research Project - Securities settlement systems: delivery-verses-payment in a distributed ledger environment (March 2018). https://www.boj.or.jp/en/announcements/release_2018/data/rel180327a1.pdf

assumption that the CSD acts as the operator of the DLT network, the same principles would apply, albeit the benefits of internalisation may be less clear in a DLT context.

Q89 Do you consider that the book-entry requirements under CSDR are compatible with security tokens? Yes/No/Don't know/no opinion.

Q89.1 Please explain your reasoning.

The concept of book-entry form under CSDR appears to be workable in the context of security token settlement on a DLT.

Article 3(1) of the CSDR provides that "*any issuer established in the Union that issues or has issued transferable securities, which are admitted to trading or traded on trading venues, shall arrange for such securities to be represented in book-entry form as immobilisation or subsequent to a direct issuance in dematerialised form*". Security tokens are (typically) inherently dematerialised and should thus meet this book-entry requirement. However, it would be helpful if European regulators produced guidance to confirm that securities recorded on a DLT ledger fall within the meaning of securities issued in "dematerialised form" that fulfil the book-entry requirements.

Article 3(2) requires that where a "*transaction in transferable securities takes place on a trading venue, the relevant securities must be recorded in book-entry form in a CSD on or before the intended settlement date, unless they have been so recorded*". The requirement to record the security tokens in book-entry form does not appear to be inconsistent with DLT based records.

In light of Recital 11 according to which the Regulation does not intend to "impose one particular method for the initial book-entry recording, which should be able to take the form of immobilisation or of immediate dematerialisation", The only constraint imposed by the regulation is that this recording on an account should take place via an authorised central depository.

CSDR therefore does not oppose the recording of security tokens in the central depository taking place via a DLT network and not via an account as understood from an accounting viewpoint. However, routing via the intermediary represented by the CSD remains an obligation. As things stand at present, a platform listing security tokens should therefore perform settlement and delivery either via another market participant authorised as CSD or by being itself authorised as CSD.

Although some Member States have considered CSDR book-entry requirements compatible with security tokens, what a book-entry system really means in a DLT environment needs some clarification.

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

Two key issues arise in the context of national law systems, both of which are already problematic in the context of today's post-trade infrastructure, and both of which might potentially pose even greater challenges in the digital assets space.

First, Member States appear in practice to be adopting divergent views on what constitutes "transferable securities" under MiFID II. Divergent views represent serious reputational and operational risks for post-trade infrastructure seeking to develop settlement, custody and asset servicing products in general, and particularly for crypto-assets. Therefore, we would welcome clarity on taxonomy and regulatory classification of a crypto-asset.

Secondly, certain domestic law restrictions exist, such as:

- A requirement to have securities in physical form; and
- Restrictions (in corporate law) on freedom of issuance, which is seen as a significant barrier to new entrants;

For company laws in various jurisdictions, it is unclear whether security tokens are share capital (and which laws and accounting treatment of share capital should apply, or voting or dividend rights). There is also a lack of clarity regarding the applicability of laws on ownership of dematerialised securities and contract laws in the context of DLT.

In order to fully benefit from the potential of DLT based systems to reduce costs and frictions in post trade, it would be welcomed if the above barriers could be addressed. This will also be beneficial for current securities holding systems.

In some jurisdictions, law and regulators facilitate the use of DLT solutions. However, EU financial law prevents them from taking further measures aimed at promoting DLT use in financial services. As such, regulatory flexibility with respect to targeted EU rules hindering the development of DLT ecosystems at national level (e.g. through an exemption/sandbox mechanism) is needed.

An important factor leading to the segmentation of national capital markets across Europe is the existence of nationally based issuer CSDs, coupled with differences and complexities in access requirements. One of the objectives of CSDR was to achieve increased competition in the provision of services by issuer CSDs to issuers, and to encourage the development of issuer CSDs that can offer services to issuers from many countries. With respect to these objectives, CSDR has had very little effect, with very few CSDs currently being able to offer services to issuers on a cross-border basis.

One significant reason is the complexity and cost of the CSDR process for the authorisation of such services, as set out in Articles 23 and 49 of CSDR. This specific CSDR process is much more burdensome than the standard "passporting" process under most European legislation.

The review of CSDR should lead to measures to increase competition between CSDs. One specific measure should be to bring the CSDR "passporting" process into line with the approach taken by other pieces of European legislation.

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 a "strong concern".

- Rules on settlement periods for the settlement of certain types of financial instruments in a securities settlement system (2)
- Rules on measures to prevent settlement fails (3)
- Organisational requirements for CSDs (3)
- Rules on outsourcing of services or activities to a third party (4)
- Rules on communication procedures with market participants and other market infrastructures (3)
- Rules on the protection of securities of participants and those of their clients (2)
- Rules regarding the integrity of the issue and appropriate reconciliation measures (2)
- Rules on cash settlement (3)
- Rules on requirements for participation (3)
- Rules on requirements for CSD links (3)
- Rules on access between CSDs and access between a CSD and another market infrastructure (3)
- Other (including other provisions of CSDR, national rules applying the EU acquis, supervisory practices, interpretation, applications…) (3)

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

The principles set out in CSDR are conceptually workable in the context of a CSD operating in a DLT environment. However, interpretative clarifications may be needed on the following:

i. Rules on outsourcing of services or activities to a third party

In a DLT environment, it is possible that some functions are not performed by a central entity (traditionally a CSD), but are performed by other actors, either alone or in collaboration. This is especially relevant where the mining or recording of transactions and the establishment of a consensus to validate a transaction can be performed by different processes and actors. In this context, clear guidelines must be established on the parameters and criteria for the outsourcing of such functions, and what roles the CSD must retain, or how some of the functions performed should be understood in a distributed environment or network.

ii. Rules on communication procedures with market participants and other market infrastructures

Platforms should be interoperable. Further consideration should be given to promote common standards that could enable interoperability between different DLT implementations and existing systems and financial infrastructures.

iii. Rules on cash settlement

Most CSDs offer settlement in central bank money, in accordance with the relevant IOSCO principles, also enshrined in CSDR. Article 40 of CSDR requires CSDs, for transactions denominated in the currency of the country where the settlement takes place, to settle the cash payments of its securities settlement system through accounts opened with a central bank, where practical and available. In a decentralised construct, it may be practically difficult to identify the country where the settlement takes place. Therefore, we find that settlement is deemed to have taken place in the jurisdiction where the DLT operator is authorised and governed, as today.

Where the cash payment is executed on a DLT network, the provision of settlement in central bank money in a DLT environment will be an important aspect for consideration. Presently, central bank money is not directly issued on DLT, however some central banks are revamping their RTGS systems to allow connection to DLT infrastructures.

Regulators and Central Banks should ensure that a DLT-based CSD could have the same level of central bank access and same access requirements as an equivalent traditional CSD, and that the rules applying to credit institutions providing banking services to current traditional CSDs also apply to DLT based CSDs.

iv. Rules on requirements for participation

See point (iv) in our response to Q 93.

v. Settlement discipline - settlement fails

Whilst recognising that DLT can drive settlement efficiency, we wish to make clear that settlement fails could still arise in a DLT context, for similar reasons to traditional CSDs. For example:

- Technology issues;

- 'Fat-finger' error;
- Lack of credit or prefunding;
- Mismatching; and
- Lack of security tokens

In a DLT context, it is conceivable that the entity performing the operator role would be able to monitor settlement fails.

vi. Settlement finality

Article 39 of CSDR sets out obligations of the CSD relating to settlement finality, including to:

- Ensure that its securities settlement system offers adequate protection to participants;
- Ensure that its securities settlement system defines the moments of entry and irrevocability of transfer orders in that securities settlement system;
- Disclose the rules governing the finality of transfers of securities and cash in a securities settlement system;
- Take all reasonable steps to ensure that finality of transfers of securities and cash is achieved either in real time or intra-day and in any case no later than by the end of the business day of the actual settlement date; and
- Settle all securities transactions against cash between direct participants in a securities settlement system operated by the CSD and settled in the securities settlement system on a DvP basis.

For security tokens, we would consider 'settlement' to occur at the point when consensus has been reached according to a predefined methodology. Accordingly, we see no inherent challenges with the concept of settlement finality in a DLT security settlement environment.

vii. Rules on requirements for CSD links., access between CSDs and other market infrastructures

While the principles behind the detailed rules on CSD links in terms of access are relevant in a context of DLT platforms connecting to each other and to traditional CSD platforms, there may be a need to review how all these rules apply in practice and whether they can all be fully implemented as such. Given that the technical platforms may be very different, any links may be complex to establish or create unnecessary risks.

Interoperability between FMIs should also apply in the context of DLT platforms.

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

AFME has not responded to this question.

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 a "strong concern".

- Definition of a securities settlement system (2)
- Definition of a system operator (3)
- Definition of a participant (1)
- Definition of an institution (1)
- Definition of transfer order (2)
- What could constitute a settlement account? (2)

- What could constitute collateral security? (2)
- Other

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?

The Settlement Finality Directive (SFD) prescribes the legal requirements designed to ensure finality in the settlement process of a designated system. The SFD provides that transfer orders entered into a designated European payment and settlement system cannot be revoked or invalidated, even in the event of the insolvency of a system participant. This is to protect the other participants in the system, and the integrity of the system itself, so that they can rely on the fact that the transfer orders entered into the system are eligible for further settlement, i.e. matching and final settlement. The SFD also provides that the rights of holders of collateral security shall not be affected by insolvency proceedings against the provider.

We find that a DLT security settlement system should be able to meet the threshold requirements to obtain designated status under the SFD, and accordingly transfer orders in respect of that system ought to be capable of applying for and attracting SFD protections for the transfers facilitated by such a system.

It is not possible to discuss whether or not DLT generically fulfils the regulatory requirements for finality of securities settlement, given this is factually dependent on how the DLT system is designed (as it would be in case any other technology is used). However, there remain various observations when considering the application of SFD to DLT networks:

- **System operator:** an SFD designated system must have a system operator, i.e. the entity legally responsible for the operation of the system. In most cases that is likely to be CSD as per above; and

- **Moment of entry of a transfer order:** the fact that there may be a distributed underlying database does not present a material challenge, because it is for the system operator to define the moment of entry in its rules, depending on the technical implementation and definition of consensus mechanisms. However, this presents a new set of considerations for European regulators to contend with. To provide a non-exhaustive list of examples, the system operator would need to clarify the position in the case of a conditional transfer order and whether it is sufficient that at least one node had correctly verified the instruction as valid in accordance with the rules of the system for the transfer order to meaningfully be said to have 'entered into the system' or whether the transfer order must be verified by all nodes, and what verification means in a DLT context.

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

We set out below our key observations on the definitions, where we would welcome that clarification from European regulators:

i. *Definition of a securities settlement system*

The SFD does not contain a definition of "securities settlement system". Instead, SFD defines a "system" - see our response to Q 93.1.

ii. *Definition of a system operator*

See our answer to Question 93.1.

iii. *Definition of transfer order*

SFD defines 'transfer order' as "*any instruction by a participant to place at the disposal of a recipient an amount of money by means of a book-entry on the accounts of a credit institution, a central bank or a settlement agent, or any instruction which results in the assumption or discharge of a payment obligation as defined by the rules of the system (a payment transfer order), or an instruction by a participant to transfer the title to, or interest in, a security or securities by means of a book-entry on a register, or otherwise (a security transfer order)*".

In line with our answer to Q 93.1, the technological implementation of a DLT settlement system would need to be designed in such a way that the implementation of a transfer order in its register complies unequivocally with the above definition.

AFME considers that the arrangement might operate as follows. We assume that in the DLT context, the CSD will be informed through a technological mechanism that Participant A on a DLT network intends to transfer its ownership of security tokens to Participant B ("the instruction"). Upon receipt of the instruction, the CSD will check that Participant A and Participant B are the eligible owners and recipients of the security tokens/cash tokens, and the CSD will take the necessary step of approving the transfer, following which the distributed ledger is then updated.

To ensure alignment with the definition of 'transfer order' in CSDR, however, it would be helpful for there to be clarification from European regulators regarding the definition of payment transfer order, in relation to how a cash leg of crypto-asset transfer would satisfy the definition of money and thereby constitute a payment transfer order with equal discharge of obligations from a legal perspective

iv. *Definition of a participant and definition of an institution*

SFD defines 'participant' as "an institution, a central counterparty, a settlement agent or a clearing house" (each with respect to the relevant designated system). An 'institution' is defined as broadly a credit institution, an investment firm (other than an exempt person under Article 2 of MiFID II), a public authority or publicly guaranteed undertaking or certain other undertakings treated as an institution.

In the same way that electronic access to centralised CSD platforms today is restricted using software, a decentralised platform can also be successfully restricted to comply with the requirement of restricting CSD participation. On this basis, and assuming the technological solution that is deployed is robust, we see no inherent challenges with these definitions, for example using a permissioned network in which only authorized parties can participate.

v. *Definition of a collateral security*

There would appear to be no inherent challenges with the definition of collateral security, assuming that crypto-assets constitute property and it is possible to take security over them.

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? Please explain your reasoning.

We find that there is need for clarification when applying these rules in a DLT network.

The SFD refers to rights "*legally recorded on a register, account or centralised deposit system located in a Member State*". Where the securities register is stored on a distributed ledger, however, the physical location of the technology holding that register is not a meaningful concept, as it could be stored on every node in the DLT network. We find that the governing law should be determined by the location of the central authority, such as a CSD, who operates the DLT network.

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

AFME has not responded to this question.

Q 96 Do you consider that the effective functioning and/or use of the DLT solution is limited or constrained by any of the SFD provisions? If yes, please provide specific examples (e.g. provisions of national legislation transposing or implementing SFD, supervisory practices, interpretation, application…). Yes/No/Don't know, no opinion. Please explain your reasoning.

The effective functioning of a DLT solution should not be limited by the SFD provisions, as long as certain terms and definitions are clarified to be technology agnostic.

Please refer to our response to Q 93.1.

Q 97-104: AFME has not responded to these questions.

Q 105 Are the provisions of the EU AIFMD legal framework in the following areas 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".

- AIFMD provisions pertaining to the requirement to appoint a depositary, safe-keeping and the requirements of the depositary, as applied to security tokens; (4)
- 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; (4)
- 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; (3)
- AIFMD requirements that appropriate and consistent procedures are established for a proper and independent valuation of the assets; (3)
- Transparency and reporting provisions of the AIFMD legal framework requiring to report certain information on the principal markets and instruments. (3)

105.1 Please explain your reasoning (if needed).

In filling in the table for Q105 our key assumptions include:

- The definition of a security token is aligned to the definition of a financial instrument as defined in MiFID;
- A 'security token' is not always a custody asset under AIFMD, and can in some cases be a "other asset"; and
- Other forms of crypto-asset (utility token or payment token) are not financial instruments and are therefore "other asset" under AIFMD.

Q 106 Do you consider that the effective functioning of DLT solutions and/or use of security tokens is limited or constrained by any of the AIFMD provisions? Yes/No/Don't know.

106.1 If yes, please provide specific examples with relevant provisions in the EU acquis. Please explain your reasoning (if needed).

From a crypto-asset perspective, AFME believes that not all security tokens (i.e. crypto-assets which meet the definition of a financial instrument under MiFID) would be "financial instruments which can be held in custody" under AIFMD, and a number of security tokens could fall into the definition of "other assets" under AIFMD. Ultimately, provided a security token is capable of being exchanged between parties, it will be a custody asset or 'other asset' based on whether the asset is registered in the name of the depositary or the fund and whether the asset (in the case of transferable securities) is recorded on the books of a CSD or other entity such as a registrar.

The challenge in either case will be that the rules - Article 89 and 98 or 90 of the AIFMD delegated regulation, require the depositary or delegate to verify AIF's ownership of the relevant security token (legal or beneficial). This obligation may be difficult to meet in practice due to the complexity regarding the integrity of a DLT platform being used in each case. Ownership of securities is usually, but not always, evidenced through the recording of the holding on the books of an external legal entity such as a registrar, custodian or CSD. In the case of a DLT platform, it is fundamental in ensuring that any recording of crypto-assets is done adequately, safely, and under strict controls to allow the depositary to apply adequate controls on ownership.

The ability to perform and demonstrate due care and protection, adequate organisational arrangements and reconciliations are conducted on a regular basis to any entity downstream by the depository is fundamentally linked to the form and legal structure of the DLT platform. For DLT platforms that either do not have a legal form and/or are not subject to such controls and supervision, it can be challenging to extend the protection afforded by AIFMD and UCITS and the oversight duties and depositary liability of the depositary under the above rules to assets held on such platforms.

The Commission may wish to provide further clarity on whether the depository can discharge liability for custody assets to the operator of the DLT if/where such an entity exists.

Otherwise, the due diligence obligations in respect of custody assets are onerous or may be impractical to perform (for example, who would the depositary perform due diligence on if there is no legal entity operating the DLT platform).

Crypto-assets which do not meet the definition of financial instruments would fall into the definition of "other assets" within AIFMD; as would security tokens which do not meet the definition of "financial instruments which can be held in custody" under AIFMD. In such cases the depositary, at a minimum, must possess sufficient and reliable information for it to be satisfied of the AIF's ownership right, and ensure that there are procedures in place so that registered assets cannot be assigned, transferred, exchanged or delivered without the depositary or its delegate having been informed of such transactions.

However, the asset verification rules are strict and raise similar challenges to the custody verification rules. The liability standard for asset verification is negligence / wilful default, but to mitigate this, the depositary must demonstrate a detailed understanding of the DLT, the rules in place within the system and the extent to which there is any 'supernode' or validating entity.

We also believe that global asset gatherers running regulated products often see UCITS/AIF eligibility as a pre-requisite for any security tokens, to aid overall liquidity and allow them to operate standard portfolios across a range of products.

We do not believe that the AIFMD provisions regarding AIFM systems and controls and liquidity management raise wholly new regulator concerns beyond those applicable to existing assets, held by AIF. This is particularly the case with respect to security tokens where the asset is 'a real financial asset' e.g. where a blue chip or tech corporation issues a

further round of debt in the form of a crypto-asset, but would be more challenging in respect of utility tokens or payment tokens.

AIFMD already accommodates a wide range of assets including leveraged loans, fine wine, art, shipping, and rules require managers not to invest in any asset without an appropriate understanding of the risks, including liquidity risks, associated with that investment, and being able to demonstrate the ability to value and monitor the asset on an ongoing basis. Where AIFs invest in cryptocurrency or utility tokens it is likely that bespoke models will need to be used to value assets as per Section VII of the AIFMD delegated regulation. This would require individual review and the AIFM could not solely use prices from a single counterparty or broker.

Q107 Do you think 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".

AFME has not responded to this question.

Q 108 Do you think that the EU legislation should provide for more regulatory flexibility for stakeholders to develop trading and post-trading solutions using for example permissionless blockchain and decentralised platforms? Yes/No/Don't know no opinion.

108.1 If yes, please explain the regulatory approach you favour and why.

AFME believes that EU legislators should consider how regulatory requirements can be fulfilled in a proportional and flexible way with due consideration to how regulations could be complied by utilising novel technological capabilities. This should also apply to the development of post trading solutions using permissionless DLT networks.

We support that there are various benefits to permissionless blockchains and decentralised technologies. A key consideration for using these technologies is to manage any arising risks in a safe and appropriate manner.

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

AFME has previously outlined benefits of DLT in Q 10 and Q 55. It is important that the EU regulatory framework remains technology agnostic (to the extent possible) and future proof in order to encourage innovation and foster a level playing field. As such, we would support leveraging existing frameworks where applicable and receiving guidance and principles rather than focusing on specifics about a network or a technology (e.g. permissioned versus permissionless networks).

However, we acknowledge that the design of the network will impact the feasibility and alignment with regulations and guidance as this technology continues to evolve.

Q 110 Do you think that the regulatory separation of trading and post-trading activities might prevent the development of alternative business models based on DLT that could more efficiently manage the trade life cycle? Yes/No/Don't know/no opinion.

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

AFME finds that DLT may someday streamline financial transactions by merging currently disparate processes such as pre and post trade. However, the current separation of trading and post-trading activities would not immediately prevent

the future development of alternative business models and until the technology matures and is fully tested, remains core to the financial services industry.

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

AFME has not responded to this question.

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

AFME has not responded to this question.

C. Assessment of legislation for 'e-money' tokens

Q 113 Have you detected any issue in EMD2 that could constitute impediments to the effective functioning and/or use of e-money tokens? Please provide specific examples and explain. Yes/No/Don't know.

AFME requests clarification regarding which activities need to take place in the EU for an EU E-money license to be needed, including the currency denomination of the asset.

Further, the definition of e-money under EMD2 is not sufficiently clear. For example, what is meant by a "claim" on the issuer and what is meant by "accepted"? The current uncertainty may capture many token structures that are not intended to be regulated as e-money. Equally, the current lack of clarity in interpreting the term "instruments of payment" leaves a residual technical risk with regard to the definition of a transferable security.

Q 114 Have you detected any issue in PSD2 that could constitute impediments to the effective functioning and/or use of e-money tokens? Please provide specific examples and explain

AFME has not responded to this question.

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

AFME has not responded to this question.

Q 116 Do you think the requirements under EMD2 would be appropriate for "global stablecoins" (i.e. those that reach global reach) qualifying as e-money tokens? (1 - 5 completely appropriate)

- Initial capital and ongoing funds
- Safeguarding requirements
- Issuance
- Redeemability

- Use of agents
- Out of court complaint and redress procedures

116.1 Any other necessary requirements?

AFME has not responded to this question.

Q 117 Do you think that the current requirements under PSD2 which are applicable to e-money tokens are appropriate for "global stablecoins" (i. e. those that reach global reach)? (Completely agree- completely disagree)

AFME has not responded to this question.

AFME contacts

Andrew Harvey, aharvey@gfma.org	+44 (0)20 3828 2694
David Ostojitsch, david.ostojitsch@afme.eu	+44 (0)20 3828 2761
Emmanuel Le Marois, emmanuel.lemarois@afme.eu	+44 (0)20 3828 2674
Madeline Taylor, madeline.taylor@afme.eu	+44 (0)20 3828 2688

About AFME

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society. AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is listed on the EU Register of Interest Representatives, registration number 65110063986-76.