UK Finance response to the FCA's discussion paper on Distributed Ledger Technology

By: Matthew Field, Policy Advisor - Digital

(matthew.field@ukfinance.org.uk)

UK Finance is the trading name of NewTA Limited. Company number: 10250295. Registered address: Pinners Hall, 105-108 Old Broad Street, London, EC2N 1EX

Guiding principles

At the outset, we consider that there are some guiding principles that are helpful to keep in mind when assessing the legal and regulatory considerations relating to distributed ledger technology (DLT). These are set out as follows:

- *A flexible and pragmatic approach* – DLT is at an early stage of development and deployment and it is important that any regulatory approach to DLT does not implicitly limit or constrain firms' ability to test and develop DLT solutions. Any specific regulatory response to DLT should be fully considered and highly informed, formulated in collaboration with the industry, demonstrably necessary based on evidence, and proportionate to the consideration being addressed. Furthermore, if a situation arises where the use of DLT to perform an activity could pose a challenge to compliance with a particular regulation, we would advise policymakers to be pragmatic in resolving such situations; the possibility of DLT-based innovation challenging an existing regulation should not necessarily be viewed negatively, given that the current regulatory framework was constructed without taking account of the development of DLT.

- *Technology neutrality and activity-based regulation* – In principle, we consider that DLT should be recognised as a foundational technology which can be used to undertake financial services activities and which could change the market structure for financial services and which could change market infrastructure for financial service, rather than as an activity in and of itself. As a consequence, while there may be aspects of the regulatory framework relevant to DLT as a technology platform, UKF considers that this is distinct from applying a regulatory framework to a regulated financial activity that utilises DLT.

  The potential uses for DLT are numerous and diverse. The regulatory framework needs to be sufficiently cognisant of the diverse potential applications of DLT that are adaptable to operating across multiple activities and services. Consequently, the adoption of a "one size fits all" regulatory framework for DLT is not likely to be effective or proportionate, nor will it further the FCA's statutory objective of fostering innovation.

  Furthermore, it is important that unregulated functions do not become regulated solely as a result of the deployment of DLT. While it may be the case that DLT could be used to perform an unregulated function in an inappropriate manner, the use of DLT per se should not be the principal driver of regulatory action in such cases, and any such regulatory action should be determined on a case-by-case basis..

- *Harmonised international approach* – DLT by its nature is distributed. Existing public DLT networks can be seen operating across many jurisdictions, as the technology is not limited by geographic boundaries or by a single legal and regulatory regime. Therefore, any requirements should be based on harmonised international standards.

To the extent that DLT forms the basis for a market infrastructure the FCA should be mindful of existing global standards and bodies, such as the CPSS-IOSCO Principles for Financial Market Infrastructures (PFMIs), which may provide a useful supra-national framework for determining the appropriate regulatory construct.

Key points:

Differentiation of private (permissioned) and public (permissionless) distributed ledger applications.

Members hold in common the view that in the short and medium term, focus by financial service providers will remain on permissioned ledgers (KYC and data protection policy compliant) as they are the more realistic and practical approach with regards to some of governance issues that might occur when DLT is applied to financial products and services.

In the medium to long term, permissioned DLTs may lead to hybrid systems with access to non-financial services participants offering variables such as access to permissioned blocks where only those with the cryptographic keys may inspect individual messages or transactions.

The Importance of Networks

Members agree that network effects are one of the key factors in the the success of any DLT application.

Networks will be essential to the development of distributed ledger technology because of their ability to operate at global scale and complexity. A major advantage of DLT is the potential to simplify at scale. For this to be successful it requires a holistic view across functions, organisations and geographies that only exist in large organisations.

However, access conditions to participants (including AML and KYC requirements) and achieving consensus on the appropriate level of administration and risk participants on the platform can take (and suggestions on how to mitigate those risks) are among some of the challenges that should be the subject of a robust dialogue between market participants and the FCA.

Therefore, in order to move toward an environment in which DLT solutions can be brought to market, the FCA should engage in a more active and robust way with existing market participants and networks. This includes individual firms, but also the networks which are formed as a legal entity by a consortium of participants. It is this legal entity which is initially most likely to hold, and take action to mitigate, risk. The FCA should thus prioritise its engagement with these networks, in particular, it should take an active position on emerging distributed ledgers by fulfilling the notary function as a node on the ledger.

Digital Identity

Members note the importance that DLT applications could play in the creation of a multi-sector, horizontal, open system of digital identities. There is an example of such a system which is in the final stages of development: Red Lyra (Lyra network) in Spain. While financial institutions are well positioned to identify their customers without extensive incremental effort, we are equally sensitive about relying on identity verification by other participants in the network, particularly when a participant is not a regulated entity.

In addition to the potential of DLT applications to digital identities, members identified a need to determine and codify a common standard for proof of identity. Distributed ledgers are closely tied to the concept of digital identity and with an increasing number of platforms on, or close to, the market, there is a need to clarify best practice and harmonise standards across the industry, to enable interoperability and ensure safety and soundness for end users.

We suggest that identity is an area where cooperation between industry and regulators would be beneficial both to the market and the attainment of regulatory objectives, and could also encourage the growth and use of the technology. We are aware of existing work ongoing through the UK Government Verify scheme and support that work. There are opportunities to use regulatory influence to set out a verifiable standard for KYC that helps each participant to leverage due diligence and verification processes to add value to the digital identity proposition. To the extent that each participant in the distributed ledger is still required to conduct its own due diligence and verification, there will be significantly less value in the digital identity proposition.

Digital Currencies

Though there are differences between private digital currencies (e.g. Ether, Bitcoin) and central bank digital currencies, both face hurdles that adversely impact the viability of a digital currency use case (e.g. digitizing legacy assets and the market demand for a digital currency). However, due to their differences we would recommend not to intertwine conversations on each topic as the drivers for adoption, potential ecosystem participants, implications, and required regulatory framework are vastly different.

We are expecting progress by the Bank of England and other central banks in the digital currency space and are currently aware of recent tests designed to explore the adoption of a cryptocurrency Blockchain by the DNB (central bank of the Netherlands) and of experimentation by MAS with a tokenised form of the Singapore dollar.

Although the issue is not addressed in detail in the paper, given the significant developments we see in this space members believe the FCA will not be able to remain agnostic on the use by the financial industry of digital currencies. The FCA should thus work with the industry to identify the different ways in which financial institutions may interact with digital currencies in order to clarify the regulatory responsibilities of doing so. In order to achieve this, we recommend the FCA consult on guidelines for interacting with digital currencies thereby allowing FIs to formalise risk and controls processes for such interaction.

Response to specific questions:

What new risks and opportunities does DLT present to our statutory objectives of market integrity, consumer protection and competition? Can DLT support more effective competition, financial system integrity and deliver better consumer outcomes? How can regulated firms mitigate any risks?

Do any of DLT's characteristics make it challenging to fit DLT solutions into the regulatory framework, despite our approach of 'technology neutrality'?

1. Please see above point in the "Guiding Principles" on a flexible and pragmatic approach to DLT.

2. As a network technology, DLT changes the relationship between various participants in an ecosystem. Further analysis is needed to understand the impact of the move from linear relationships to networked relationships. For example, how do obligations that currently exist for linear relationships (e.g. due diligence, KYC, AML, etc.) extend to other participants in a networked DLT ecosystem?

3. Other risks presented by DLT are similar to those which the industry has successfully managed in the past such as the potential for concentration risk in a single provider or difficulties with exit strategy caused by limited interoperability among providers. Although these can be risks for FSIs, regulators and industry participants are currently finding solutions to such questions and members encourage the FCA to look to the outcome of that process when considering DLT, which is not yet at a stage of development where these issues need to be addressed to allow progress.

Q1: How will firms demonstrate appropriate outsourcing arrangements when relying on third parties (such as core developer groups of public, permissionless networks) to deliver DLT-based solutions?

4. Existing outsourcing rules and regulations which are known to firms must be considered when substituting process to third-parties and when using federated networks. Although DLT does not fundamentally change outsourcing rules, it may raise new questions about the applicability of existing legislation to new risks or when using networked relationships.

5. An important consideration is the international and cross-jurisdictional nature of the technology. UK Finance recognises that the FCA already communicates with peers in other jurisdictions and we encourage this dialogue to continue.

6. Unlike other technologies, the interconnected nature of a distributed ledger means that entities subject to conflicting or incompatible regulatory regimes may not be able to participate in the ledger. Members believe that divergent regulation currently being introduced or developed in different jurisdictions could create unnecessary friction and slow market development.

7. Specifically, in the case of DLT, permissionless ledgers could be considered open source technology while permissioned ledgers will be provided or operated by vendors. Neither of these is outside the existing regulatory framework. The standards for robust third-party oversight and technology controls procedure would apply to any DLT solution as with any other technologies provided by a third-party.

8. We note that it should be expected that the importance of the considerations discussed above will increase as organisations progress with their use cases and the deployment and application of distributed ledgers becomes more sophisticated.

Q2: What operational risks have firms identified with (i) implementation of DLT systems (ii) system-wide issues affecting multiple firms, and how will they manage them?

9. Given that DLT is still a nascent technology, any view on the future risks involved will to some extent develop over time. In some areas the expectations for DLT applications to provide solutions may exceed the underlying technology developments. In other areas DLT applications may establish relationships that are new to the regulatory landscape or alternatively incur risks similar to those that firms must currently manage when adopting any new technology.

10. Regarding implementation of DLT, firms are aware of the need to integrate and operate with so-called legacy systems. These practical integration points will be an ongoing challenge, but again, one that the industry has successfully managed before and which should not be viewed as outside the normal scope of technology risk which must be mitigated.

11. As per above, we believe that third parties will be necessary to hold and mitigate risks in a distributed ledger. This model is similar to many currently in use in financial services today and we would once again point to PFMIs as a model to consider.

12. Firms participating on the ledger will control for risk by identifying appropriate controls and introducing them where appropriate. This is much the same as has been done in the past for new technologies and will continue to be a necessary function within FSIs. With the rapidly increasing use of technology in financial services we find that industry risk frameworks should be developed in order to ensure best practice and desired regulatory outcomes for consumers and markets. Regulatory participation and eventually recognition of such frameworks will be important to ensuring a regulatory environment which is flexible enough to ensure appropriate outcomes.

Q3: What is the best way for DLT networks to protect themselves against attempts to break DLT network security?

13. There is no single identified method of defense that can be applied across all DLT networks as different platforms have different characteristics which can be exploited and protected in different ways. That said, it is worth noting the following regarding DLT security:
    - Although in time possible, the risk of threat actors 'cracking' (i.e. retrieving the original plaintext from the hash) the industry standard cryptographic encryption algorithms is extremely low. Furthermore, we expect this would be addressed universally by the cyber security industry through market demand (especially given the widespread use of these hash algorithms in every day computing) and is not a problem limited to DLT. The FCA correctly notes that "the strength of security afforded by encryption is continually under challenge, reflecting increases in computing power and sophistication of algorithms."
    - Cyber attacks, where private key access is stolen or fraudulently used to gain access as a participant on a DLT network, are an ongoing concern. However, in a privacy-preserving model where participants only have access to the trades that they are party to, a breach of one participant's node(s) does not automatically equate to access to all other participant's data. The impact is certainly limited and is arguably no different to a cyber attack that takes place in a non-DLT environment.

14. Regarding cyber security generally, the industry supports efforts for strong information sharing to help protect against and prevent cybercrimes which would:
    - make it easier for the public and private sectors to share threat information in a timely manner;
    - allow the government to declassify cyber threat information so that it can be utilised by the private sector for their protection; and
    - provide strong liability protections for entities sharing appropriate cyber threat information.

Q4: What technology resiliency advantages, if any, does DLT have over other types of systems currently available?

15. The distributed nature of the technology means that the risk profile differs from a centrally hosted transaction platform / IT system. This means that the threats, potential vulnerabilities and risks facing DLTs are subtly different rather than being lower than 'traditional technology'. A direct parallel can be drawn with the cloud versus on-premise hosting debate in that a new context brings the need for innovative control strategies.

16. While the security of Distributed Ledgers has not yet been subject to significant, broad-based testing in the financial services industry, we can learn from the experiences of the existing cryptocurrency implementations. Attack analysis will be required to prepare for new tactics and techniques that could be used to defraud, disrupt and ultimately undermine future DLT use cases.

17. We note that in circumstance of a wide adoption and use of DLT, if a single or multiple DLT provider were to suffer technological fault, hacking or default, the consequences could be severe in the market. However, this is not an issue specific to DLT as cyber risks are already present in existing market infrastructures and blockchain-based systems have (to date) a strong cyber-security record.

18. The financial services industry is one of the most experienced at controlling for and mitigating cyber based risk. Further, in terms of recovery from an incident, the industry believes that distributed and shared nature of the system could facilitate recovery of both data and processes (assuming that not all nodes were corrupted simultaneously) possibly reducing the need for costly recovery plans.

19. Finally, members would like to bring to the attention of the FCA the importance of considering the implications of the development of quantum computing to the use of distributed ledgers. The impact of quantum on cryptography and encryption (and trading) could be felt far beyond financial services and blockchain, however, it is important to consider how DLT could be future proofed as well as what implications there might be for proposed applications.

20. We note, of course, that quantum will have just as significant impacts on traditional systems and so the issue should not be viewed as isolated to DLT.

Q5: What DLT use-cases are currently under development in the (re)insurance sector? Are there likely to be significant (re)insurance DLT deployments in the near term?

21. No response

Q6: What use cases have been live tested for regulatory reporting? What challenges are there to implementing these solutions?

22. Various solutions have been tested or are currently being testing in markets around the world. The most promising use cases of technologies for compliance purposes are:
    - identification of clients and legal persons (including ultimate beneficial owners) for the purpose of Know-Your-Customer (KYC) requirements,
    - real-time transaction reporting to regulators including for anti-money laundering (AML) and counter-terrorism financing (CTF) purposes,
    - fraud prevention, and
    - automation of compliance reporting.

23. As in paragraph 22, one advantage of DLT is the ability for regulators to monitor DLT systems in (close to) real time. We note that other regulators, including MAS and HKMA, are actively considering fulfilling a notary function on several different ledgers requiring them to be a node on the network. Though this has implications for some regulatory reporting use cases, it is not necessary for all solutions or for meaningful progress to be made in this area. The FCA should consider its appetite for such a role. It is the opinion of the industry that this will eventually be necessary for the UK to reap the full advantages of DLT.

24. Regarding the use of DLT for regulatory reporting purposes generally, ambiguity as to the comfort of the regulator and the existing regulatory regime with DLT use cases for regulatory reporting, as well as other applications, is a significant challenge to development and deployment. While there needs to be some level of engagement between regulators and industry, there is a balance to be struck between engaging too early, in case a DLT application is insufficiently developed to usefully inform the FCA, and engaging too late, in case firms have invested time and resource in an inappropriate solution.

25. We thus encourage the FCA to work with industry which, if done correctly, will allow industry to make informed development decisions while providing the FCA with an increased understanding of specific DLT applications. Such early interaction and alignment with the regulator would allow the institutions to clarify regulatory monitoring requirements in an early stage, reduce implementation risk for institutions and allow the regulator to have early sight of developments in this space so that they can calibrate their regulatory approach appropriately. As a consequence, it could significantly reduce the time to market for such DLT solutions in the UK.

26. Finally, in other tests, some of the challenges presented include ensuring the sufficient anonymity of data even in the case of public data. The industry is still in search of solutions that allow reconciliation between markets whilst keeping the necessary levels of anonymity.

Q7: How might DLT be deployed to mitigate financial crime risks, and will regulated firms adopt such solutions? If so, in what timeframe? If not, what are the barriers to adoption?

27. The nature of distributed ledgers makes it easier to track transactions and money across the network thereby creating increased data for the purposes of financial crime mitigation. These benefits would need to be balanced with the appropriate level of anonymity. It is worth noting that the use of DLT should not introduce additional money laundering risks, over-and-above those that exist in the normal course of financial services activity, so long as it is employed on a permissioned network.

28. The digital identity potential of distributed ledgers will be a key factor in any financial crime solutions presented by DLT. When combined with cryptographic consensus there is potential for DLT to provide a significant improvement to current practice in the detection of financial crime.

Q8: Is this a viable use case for DLT in the context of asset management? What other examples are there for this sector?

29. Corporate actions processing is a potential use case. In this case, processes for corporate actions events (e.g., proxy voting income distributions) across issuers and investors are streamlined via a distributed ledger. Potential benefits include reduction in administrative costs and manual processing required which can reduce errors.

30. However, there is a lack of legal certainty around, for instance, how digitised assets to be treated under law and whether they convey ownership of an underlying physical asset or if they are an asset in and of themselves (thus becoming a form of digital currency).

Q9: What other examples are there of DLT providing direct and tangible benefits to consumers? What are the risks associated with these?

31. DLT is thought to have more potential to reduce operational costs for financial service providers and/or increase their efficiency. Although these benefits may not be direct to consumers, they are tangible in the form of reduced costs and a more efficient market. Examples of these improvements are given below.

32. Real Time Payments: Today banks rely on a network of correspondent banks that allow clients to make cross-border payments on an average of a T+1 / T+2 basis (though this time period can extend depending on the location of the payee and any additional checks and compliance that must be undertaken). A number of banks have been reviewing new blockchain-based payment protocols available on the market and experimenting with a proof of concept platform. These solutions take advantage of the capabilities of blockchain to execute payment obligations netting and enable real-time clearing without the involvement of correspondent banks on each transaction.

33. Digital Cash / Utility Settlement Coin: A number of banks are currently collaborating on the concept of the Utility Settlement Coin (USC), an asset-backed digital cash settlement token implemented on distributed ledger technology for use within global institutional financial markets. USC would be multi-currency denominated, with a version for each of the major fiat currencies (GBP, EUR, USD, etc.). Unlike cash held as a commercial bank deposit, USC would be fully backed by cash assets held at a central bank. Essentially, spending a USC would be spending its paired fiat currency. The roll-out of the Utility Settlement Coin would help enable a common unit of value across different blockchain platforms in institutional markets. USC could have a wide range benefits from balance sheet implications to improved processes around clearing and settlement. The risk, complexity and time taken to settle and clear trades could also be significantly reduced.

34. Cross-border payments/Digital Trade Chain (DTC)**:** DTC is a Blockchain-based digital platform for managing and tracking domestic and cross-border Open Account trade transactions securely. The aim of the platform is to make domestic and cross-border commerce easier for European small and medium-size (SME) businesses by harnessing the power of digital distributed ledger technology. DTC will enable authorised customers to initiate transactions on a paperless but secure basis, and track the transaction at each stage of transaction lifecycle, through to the point of settlement/payment. Customers will also be able to request banking products for the transaction, such as:
    - payment Notification by the buyer's bank upon the settlement of an invoice,
    - bank payment commitment by the buyer's bank; and

- invoice discounting (forfaiting) for the supplier.

35. By maintaining secure records on a digital distributed ledger, DTC has potential to accelerate the order-to-settlement process, and significantly decrease administrative paperwork.

Q10: How do respondents see the use of smart contracts developing in financial services? Please provide examples, ideally which have been already live tested.

Terminology:

36. Smart contracts as a term is used to cover a range of "code" where "code" is a generic term defined as a "sequence of instructions to achieve a task" and therefore encompasses computer code and written contracts. Smart contracts can thus range from the very simple (e.g. code to calculate a coupon due, track assets settle, etc.) to very complex, an example of which would be how to manage the default of a party to a portfolio of derivate contracts.

37. It is important also to make the distinction between "smart contract code" and "smart legal contracts". When we talk about "smart contract code" we are referring to the technology – code stored and executed on a blockchain. The application of that technology towards augmenting or replacing legal agreements is a specific use case best referred to as "smart legal contracts".

38. Most enterprise blockchain developers are primarily interested in unlocking the benefits of "smart contract code". The split of value opportunity between simple and complex smart contracts is not fully known, however, logic would suggest the most value is in the simple end (i.e. those processes that have been "coded" in a highly repetitive manner in thousands of systems across the industry). Although smart contracts are part of how DLTs will be made useful, at this stage they are not considered a replacement for current legal contracts.

39. We note the FCA's definition of smart contracts, for the purpose of its discussion, as blockchain functionality to execute pre-determined commands without further human intervention". While we broadly agree, it is important to clarify that smart contracts can be coded to require human intervention; it's a choice to do so or not. So whilst we can achieve greater/smarter efficiency, this does not necessarily result in lower control.

Use cases:

40. In our view the use of DLT and smart contracts can potentially enhance specific businesses of the bank (e.g. trade finance and supplier chain finance) and general areas (e.g. IT Core Banking).

41. In trade finance DLTs can ensure that all parties can see and transfer shipping and trade documentation through a decentralised network, reducing friction and costs, and reducing the risk of documentary fraud.

42. In supply chain finance, DLTs can be used for invoice financing and to build a payment reconciliation engine to work together with invoice messaging, producing significantly less friction and faster transactions between buyer and sellers and their respective banks.

43. These programmable digital contracts can (upon successful verification and due diligence) self-execute and cross verify through business logic "described" by their code, relying on the underlying existing infrastructure or on blockchain exchange to exchange messages and transactions, while maintaining/updating the DL shared by every network participant. A trialled example is the Smart bond (see Q15).

Q11: Does the use of digital currencies to provide financial services carry with it different or more benefits and risks than current systems available? Are there examples of this already occurring in industry?

44. Please see our response to question 4.

45. Private digital currencies are increasingly prevalent in the P2P market, and in the financial industry tokenised forms of currency have been tested although they are not widely used outside of testing environments.

46. Central bank currencies have had limited if only experimental use. As we noted earlier, the industry expects that movement in the space of central bank issued digital currencies is imminent and thus that the FCA must

decide how it will treat their use. As above, we recommend that the FCA consult on guidelines for interacting with digital currencies thereby allowing FIs to formalise risk and controls processes for such interaction.

47. The potential risk implications of private digital currencies have been identified and are being considered by the financial services industry. These include:
    - The uncertainty on tax implications may outweigh the benefits for businesses and users (depending on the jurisdiction);
    - If considered chattel, there may be *nemo dat* issues to consider of which customers should be aware;
    - The global nature of private digital currencies and lack of common regulatory approach adds additional complexity;
    - AML: private digital currencies (e.g. bitcoin) introduce AML risks due to use anonymity and the lack of a tie to a central bank, government or regulatory framework.
    - There are security and theft risks posed by private digital currency businesses for consumers and volatility risks for investors. The extent to which these risks differ from other categories of currency or investment is still under debate.

48. There are examples where the industry is experimenting with digital currencies or digital currency-like systems. One such example is the Utility Settlement Coin (USC) project, as described above in response to Q9.

49. This project can advance blockchain development by introducing a common unit of value across different blockchain platforms in institutional markets. For instance, one bank might have its own blockchain-based platform to issue bonds, and another bank might have a blockchain-based stock trading platform, but both could use the same settlement coin. USC could have a wide range benefits from balance sheet implications to improved processes around clearing and settlement. The risk, complexity and time taken to settle and clear trades could be significantly reduced.

50. The concept was developed in partnership with a blockchain startup in September 2015 to validate the potential benefits of USC for capital efficiency, settlement and systemic risk reduction in global financial markets. The project, originally part of one bank's incubator programme, was expanded after the initial phase into a collaborative project involving several other banks and the startup. Each consortium member has project leads participating in the governance committee of the project and cross-divisional teams contributing to the development of the project.

51. During the acceleration phase the consortium members aim to adopt an iterative approach that will allow them to refine the USC model and technology as well as gather feedback from other market stakeholders, central banks and regulators. In this way they hope to be able to outline at an early stage a plan and proposal for further developments of the project. No exact timeline for commercial roll-out is set at this point.

52. This project is thus an example of the potential benefits of using digital currencies or digital currency-like systems, but also a model for how risk and governance will be managed. Like other consortiums there is a third partner in the project and the group of market participants itself often becomes an entity in order to advance the project and deal with arising issues including risk.

53. The industry would welcome the chance to explore potential uses, benefits and risks around digital currencies at greater length with the FCA. As discussed above, the question of the treatment of platforms is of particular interest to financial services in this area.

Q12: What are the benefits and risks of using a public, permissionless DLT network on an existing protocol, rather than the development of proprietary DLT protocols?

54. As explained above, in the short to medium term we consider private, permissioned ledgers as a more viable option for use in financial services.

55. In the longer term, the choice of a private permissioned or a public permissionless ledger would depend on commercial objectives. The main risks of permissionless DLT networks are:
    - KYC/AML considerations around who you are trading with. In a permissionless system, the participants are anonymous so it is not possible to complete these fundamental checks.
    - Recourse in case of contract breach or other transgression – again the anonymity makes this impossible.
    - Any trading, clearing or settlement includes a degree of counterparty risk: what if the counterparty does not deliver the goods and the market has moved? This inherent risk is the rationale behind CCPs and the DVP

mechanisms advocated by IOSCO etc. If, as on a permissionless ledger, you do not know the identity of your counterparty how can you measure/assess the degree of risk?

56. The main advantages of a public permissionless ledger would be the ability to scale and reach across markets and industries. However, this introduces significantly more questions about control and compliance as well as the ownership of risk which is why private permissioned ledgers have been the focus of current testing.

57. Other advantages to permissioned ledgers include:
    - increased security measures/reduced scope for hacking – gating the community allows strict control over who has access to data, who can trade and who has access to software etc;
    - governance of the network is simplified in terms of protocol upgrades and expansion – when you know who is on the network, you know who you need to communicate with.

58. It is important to note that there are examples of permissioned networks that are not necessarily closed or proprietary. Such networks can also be open source allowing developers to take advantage of the benefits of permissionless networks, without the major risks outlined above.

Q13: What are the risks to competition of a group of incumbents operating a closed network to the exclusion of others?

59. We do not see this as a new issue or an issue unique to DLT. There are currently a number of market infrastructures in operation which operate within a range of openness to the wider market. We believe that the paradigm of fair reasonable and non-discriminatory access would apply to financial institutions and other participants that achieve the conditions for admission into a DLT (for example KYC and AML requirements) and consensus on participants that provide node processing or system support and maintenance. General competition law considerations would also apply in respect of market dominance and agreements between undertakings. Accordingly, we do not foresee this as a major hurdle. It seems more productive to emphasise that the point of operating a closed network is to mitigate systemic, operational, and technological risks for participants and end consumers / investors, as highlighted previously in our arguments for a permissioned network.

Q14: Where should responsibility lie in fully decentralised applications such as the DAO? What governance arrangements do firms plan to have in place when using applications on public, permissioned networks?

60. Such use cases remain largely untested at this stage among our membership. Uncertainty in liability allocation on a public, permissionless DLT network is one reason amongst others, why members are of the view that any deployment of DLT within financial services is likely to be of a “permissioned” network. See above for further comments on the suitability of permissioned versus permissionless ledgers and the role of platforms.

Q15: Do firms see the above examples as realistic use cases for DLT in securities issuance and trading?

61. In the near term it is possible that there will be more applications in the clearing of trades, and reconciling of information rather than the transfer of value. This is due to detected complexities in converting legacy assets to a digital format, the lack of a digital central bank currency and scalability challenges associated with the vast amounts of data associated with settlement. There may also be regulatory hurdles relating to privacy.

62. An example provided by a member of a use of DLT in securities issuance and trading:

<u>Smart Bond:</u>

63. One firm has conducted an experiment with a smart bond using blockchain and smart contracts. The experiment aimed to validate the feasibility of the overall blockchain approach and the initial smart contracts hypothesis. The firm took a popular financial instrument, a simple bond, and tried to model its logic and lifecycle on blockchain.

64. To do this, they built an experimental application on an enterprise blockchain that can recreate the issuance, indication of interest, coupon payments and maturation of a bond. In this simple experiment, the bond issuer and the bond buyer can easily execute their trades (e.g. publish their offers and indications of interest on blockchain) by using the interface the firm build on the blockchain. In addition, the issuer and the buyer don't

need the support of pre and post-trade intermediaries, as the smart bond contracts and the blockchain are able to manage automatically and almost instantaneously the flow of information and money.

65. Running this experiment the firm also had the chance to improve their knowledge of digital currencies as they had to create a private digital coin to support the exchange of money between the issuer and the buyer, which for simplicity they referred to as BondCoin. The coin is not a "digital only" crypto currency like Bitcoin, as in a real scenario it would be directly linked to fiat currency and connected to central bank accounts, meaning that an institution spending the coin would be spending real money.

66. Even if this was just an experiment, it allowed the firm to consider the potential benefits of the full implementation of a Smart Bond platform. For their clients, the platform would enable a more convenient way to issue bonds, with lower administrative costs and increased speed of issuance and investor response. For the regulator, the platform would allow real time visibility into securities positions and therefore a more precise systemic risk overview. In addition the regulator would be able to sign the business logic of a smart contract in advance, guaranteeing that products will only be sold as intended. And finally for the firm itself this would mean reduced risk from real time clearing and settlement as well as reduced cost on clearing and settlement which would also impact the price structure.

67. With regard to the use cases described by the FCA in the discussion paper:
    - Model A is a distributed ledger used for internal record keeping purposes by a single firm – for large firms with multiple subsidiaries and complex requirements, e.g. intra-firm transfer pricing models, this model may yield significant enough benefits to be deployed. There appear to be no particular obstacles to such a use from a regulatory perspective.
    - Model B is a DLT-enabled transaction processing and settlement platform that is similar to the current process for payments and securities transaction clearing, which involve tracking of transaction confirmations / settlements between market participants, with final settlement occurring at the “fiat” level or at a central clearinghouse that provides the underlying “rails” to facilitate settlement finality at EOD. Given that this use case incorporates currently-accepted “rails” to final settlement and can provide significant efficiency benefits, it seems like a realistic DLT application.
    - Model C involves using a third-party digital currency to settle payments related to the purchase and servicing of assets. Such a model is technically feasible in our opinion, but we have not seen a case that has the sufficient legal and regulatory backing to replace or integrate with the role of fiat currencies in existing financial infrastructure.

Q16: What legal and regulatory challenges do firms find in fitting initial coin offerings into our regulatory framework?

68. As the prevalence of ICOs increases it will become necessary for the FCA to set out its position on whether firms can have such currencies on their books. We recommend the FCA consult with the industry specifically on the regulatory considerations for interacting with ICOs and holding such instruments on firms’ books.

69. Currently there is a significant level of uncertainty as to the application of existing regulation. The regulatory challenges to be addressed include:
    - The characterisation of the ICO scheme and applicable regulatory framework (software pre-sales vs securities offerings)
    - Duties and obligations of the scheme operators
    - AML implications
    - Consumer protection

Q17: Are there other parts of regulation where DLT might offer a new market convention?

70. In general, in cases where DLT does offer a new market convention we would point out again that it would not be DLT itself, but a DLT application or DLT based solution which may do so.

71. If such a situation poses challenges within a certain regulation, policy makers should take a pragmatic approach to such situations. The possibility of a DLT application not fitting within certain regulations should not be viewed negatively given that the current regulatory framework did not contemplate the use of technologies like DLT.

72. That pragmatic approach should aim to regulate the application/function being deployed via DLT, rather than the technology itself. The uses for DLT are numerous and diverse and the adoption of a “one size fits all” regulatory framework for DLT is unlikely to be effective or proportionate. The regulatory framework needs to be sufficiently adaptable to operate across the multiple applications of DLT. Therefore, the technology itself should not be regulated. Related to this, it is important that un-regulated functions do not become regulated functions solely by virtue of their reliance on a DLT-based solution. Any regulatory action in such cases should be determined on a case-by-case basis, rather than the sole determining factor being the underlying use of DLT.