Reply form for the Discussion Paper on Distributed Ledger Technology

Error! Unknown document property name.

Date: 17 July 2017

Responding to this paper

We are asking for comments on this Discussion Paper by 17 July 2017.

You can send them to us using the form on our website at:
www.fca.org.uk/dp17-03-response-form.

Or in writing to:
Chris Kiew-Smith Strategy and Competition Financial Conduct Authority 25 The North Colonnade Canary Wharf London E14 5HS

Telephone: 020 7066 1040
Email: dp17-03@fca.org.uk

We have carried out this work in the context of the existing UK and EU regulatory framework. We will keep it under review to assess whether any amendments may be required in the event of changes in the UK regulatory framework, including as a result of any negotiations following the UK's vote to leave the EU.

We make all responses to formal consultation available for public inspection unless the respondent requests otherwise. We will not regard a standard confidentiality statement in an email message as a request for non-disclosure.

Despite this, we may be asked to disclose a confidential response under the Freedom of Information Act 2000. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the Information Commissioner and the Information Rights Tribunal.

You can download this Discussion Paper from our website: www.fca.org.uk. All our publications are available to download from www.fca.org.uk. If you would like to receive this paper in an alternative format,
please call 020 7066 9644 or
email: publications_graphics@fca.org.uk or
write to: Editorial and Digital team, Financial Conduct Authority, 25 The North Colonnade, Canary Wharf, London E14 5HS

Executive Summary

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to share our views on the Discussion Paper issued by the Financial Conduct Authority on Distributed Ledger Technology published in April 2017 with a deadline for a response by 17 July 2017.

Please do not hesitate to contact Emmanuel Le Marois on 44 203 828 2674, email Emmanuel.LeMarois@afme.eu, or David Ostojitsch on 44 203 828 2761, email David.Ostojitsch@afme.eu, should you wish to discuss any of the points.

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.

- AFME believes Distributed Ledger Technology (DLT) can deliver a more competitive and innovative financial sector due to the **long-term benefits that will arise from the adoption of DLT** such as:

  i) **More efficient post-trade processes**;
  ii) **Enhanced reporting and supervisory functions**;
  iii) **Greater availability and security**;
  iv) **Reduced counterparty risk** and enhanced collateral management.

- AFME believes adoption of DLT in the context of financial markets should be based around the following principles:

  i) **Only a "private and permissioned" DLT** will provide for the level of control and trust required for financial market users;
  ii) **Regulation should focus of the activity taking place** not the technology that delivers it;
  iii) **Establishing a governance framework** that supports a resilient, efficient and competitive use of DLT;
  iv) **A strong focus on standards**, such as a universal standard for reference data, **and interoperability** will speed adoption and drive collaboration;
  v) **Additional efforts should be considered to promote and facilitate member access to the technology** that complement adoption and benefits of DLT.

- AFME believes that the regulatory stance towards DLT has particularly important implications for its development and should focus on the following:

  i) To realise the benefits of DLT, **AFME believes a strong collaboration between regulators and industry participants is required**;
  ii) As DLT technology evolves, **regulators should monitor for emerging risks and act when warranted**, while ensuring there are no constraints on collaboration within the ecosystem. Engagement beyond this may have unintended consequences;
  iii) **Any new regulatory framework should seek international harmonisation, be flexible, graduated and principles-based, and oversight should be tied to scale and the risks presented**.

- AFME members feel **that significant challenges remain** before wide scale adoption of DLT is achieved due to legal, regulatory, technical and operational factors.

1. DISTRIBUTED LEDGER TECHNOLOGY: RISKS AND OPPORTUNITIES

1.1. Governance and technology resilience

Question 1:

- *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?*

Currently, financial market actors are required to comply with outsourcing arrangements as defined by MiFID[1] in 2006. These standards require banks to comply with robust controls and to review those processes currently in place for DLT, ensuring that they are the same as those employed for any other service or technology provided by a third-party. However, AFME believes that there is further opportunity to review and harmonise, especially considering recent technology developments and their potential impacts on the industry. AFME notes that national regulators have issued guidelines and recommendations on outsourcing which has led to a fragmentation of the European landscape: see guidelines issued by Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)[2], Autorite des Marches Financiers (AMF)[3], Luxembourg for Finance[4] or the Central Bank of Ireland (CBI)[5].

Furthermore, AFME believes that the question posed by the FCA requires further clarification. Due to the decentralised nature of DLT, third-party risks have specific considerations to bear:

i) **Network design**: AFME believes that DLT adoption within the securities market could only be based around a private and permissioned design, with adherence to a rigorous governance framework. Therefore, even if the underlying "code" supporting the network is from an open source model, its implementation on a private and permissioned network would have to adhere to the rules and controls defining the network;

ii) **Global Collaboration**: While collaboration amongst nodes is implicit on a DLT network, collaboration between DLT solutions may have to be devised to ensure interoperability across jurisdictions. However, any new entrant including another network, would have to adhere to the rules and controls defined by the private and permissioned design;

iii) **Interoperability**: Financial market actors will have to design DLT solutions to incorporate the current technology landscape complying with regulatory requirements. Incorporating DLT solutions with current IT architecture of financial markets may only be achieved in a private and permissioned network where appropriate controls can be implemented and monitored.

[1] http://www.mifidconnect.com/mifidconnect/downloads/MiFID_Connect_Outsourcing_Guide.pdf

[2] BaFin Outsourcing Link

[3] AMF Outsourcing Link

[4] Luxembourg for Finance Outsourcing Link

[5] CBI Outsourcing Link

A governance framework for DLT would further support adoption whilst striking the balance between rules, allowing for speed of processing and maintaining appropriate controls for safety and financial stability. A governance framework for DLT would have to solve for the following principles:

i) **Roles and responsibilities**: As seen by the 2016 Bank for International Settlements (BIS) report[6], a governance framework for DLT would have to consider the rights attached to each participant in the network such as (1) a system administrator acting as the gatekeeper controlling access to the system and providing certain specific services (2) the asset issuer permissioned to issue new assets (3) the proposer permissioned to propose updates to the ledger (4) the validator permissioned to confirm the validity of a state changes (5) the auditor permissioned to view the ledger but not make updates;

ii) **Vetting and approving participants**: Establish an accredited evaluation capability and an approval process that engages other network participants and relevant supervisors;

iii) **Monitoring compliance**: Establish an accredited capability for the ongoing review of network participant compliance against the governance framework and oversight of any agreed remediation actions;

iv) **Enforcing standards**: Establish a compliance review board comprising network participant appointees ensuring network participants maintain within the jurisdictional reach of the governance model as a condition of membership;

v) **Managing cross-border disputes**: Establish an independent arbitration panel and process to oversee disputes between network participants, and enshrine the legal enforceability of its decision within the rules of membership for each network participant;

vi) **Liability in the event of a cyber breach**: Although this may be applicable to cyber risks in general, DLT solutions will have to devised a mean to define, develop, and maintain a cyber resilience framework aimed at addressing current and emerging cyber threats, establish a cyber risk management capability, establish a cyber risk board amongst network participants;

vii) **Regulatory accountability**: Where relevant for certain use cases, engage relevant supervisors to agree on a framework through which regulators will ensure accountability of firms for the management of DLT functions.

Question 2:

- *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?*

Although DLT solutions present specific technological features, AFME believes that the risks posed by DLT are no different than operational risks currently managed by market actors.

[6] 6 http://www.bis.org/cpmi/publ/d157.pdf

Broadly, the following encompass the categories of operational risk that fall within set of reform measures developed by the Basel Committee on Banking Supervision or "Basel III"[7]:

i) **Internal fraud**: misappropriation of assets, tax evasion, intentional mis-marking of positions, bribery;

ii) **External fraud**: theft of information, hacking damage, third-party theft and forgery;

iii) **Employment practices and workplace safety**: discrimination, workers compensation, employee health and safety;

iv) **Clients, products, & business practice**: market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning;

v) **Damage to physical assets:** natural disasters, terrorism, vandalism

vi) **Business disruption and systems failures**: utility disruptions, software failures, hardware failures;

vii) **Execution, delivery, & process management**: data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets

AFME believes that to effectively manage operational risks within a DLT enabled securities market, the following principles should apply:

i) **Private and permissioned**: DLT solutions should be based upon a private and permissioned design with adherence to a rigorous governance framework, ensuring trust and accountability amongst participants;

ii) **Technology neutrality**: DLT remains largely untested compared to technologies that are currently prevalent. Therefore, AFME believes DLT adoption is most likely to be incremental to optimise current processes, while the technology matures, becomes scalable, and is more widely adopted. Therefore, AFME views the that the principle of technology neutrality should be maintained while the technology is tested and matures;

iii) **Collaboration**: While adoption of DLT across a broad spectrum of the financial services sector (actors, products and life-cycle) would reap the most scalability benefits, a strong governance framework and the active collaboration of all actors of the eco-system -when appropriate-, would ensure interoperability and resilience against external threats. Currently, this may only be achieved in a private and permissioned design;

iv) **Regulatory engagement**: AFME believes that continued engagement of regulators in the early development of the technology would avoid that DLT takes an unacceptable path to regulators. 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 challenges that should be the subject of a robust dialogue between market participants and policymakers. The industry would like to consider regulatory engagement at late stages of DLT

[7] http://www.bis.org/bcbs/index.htm?m=3%7C14

development in more detail with the FCA. Furthermore, cross-border applications of DLT will require global regulatory coordination to ensure these applications are developed in a safe way;

v) **Regulatory flexibility**: The regulatory framework is key to ensure that appropriate rules and controls are applicable as the technology matures. For example, the development of DLT could potentially impact the way market infrastructures operate, therefore rules should be adapted to encompass potential role changes.

AFME has identified the following operational risks for DLT implementations:

i) **Testing**: DLT technology is largely unproven at scale and remains at the stage of proof of concept, outside of a small number of specific implementations in a production state. However, while DLT is still in its early design stage this offers the opportunity to integrate lessons learned and make right by design;

ii) **Integration**: DLT solutions will have to integrate with existing IT architectures at each node, blending legacy and newer technologies, but will offer the opportunity to review IT architectures and identify areas for optimisation;

iii) **Interoperability**: DLT solutions arising from different jurisdictions and actors will have to devise means to ensure interoperability between different DLT solutions, for actors operating globally on multiple platforms. AFME believes that interoperability between DLT solutions may only be achieved through a private and permissioned design, which would allow for effective controls and collaboration amongst participants and networks;

iv) **Privacy**: DLT solutions may potentially offer access to information stored on a ledger directly to participants, such as regulators, increasing transparency of information. However, for confidentiality purposes, data stored on a DLT will require careful partitioning and encryption. Currently, this may prove challenging to achieve outside a private and permissioned design;

vi) **Fraud**: The risk of money laundering and transaction fraud may be exacerbated on a DLT solution due to involvement of actors across jurisdictions. However, DLT solutions are potentially more transparent and require a higher level of collaboration amongst participants. The development of digital identities may become pivotal in the development of DLT solutions as they would support efforts and regulation encompassing KYC/AML processes to date. Currently, this may only be achieved in a private and permissioned design;

v) **Cyber security**: 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 due to node distribution, the potential interconnection of networks and the use of executable code (e.g. smart contracts). 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 participants' data. The impact is certainly limited and is arguably no different to a cyber attack that takes place in a non-DLT environment. Furthermore, DLT solutions could offer higher levels of resilience due to potentially higher threat detection capabilities, as participants are bound to collaborate more, the use of encryption, the use of consensus algorithms and distributed databases, which increase resilience and data recovery capabilities in the event of a breach. However, AFME believes effective cyber resilience may only be achieved via a private and permissioned design.

Further, AFME has identified the following operational risks for system wide issues on DLT:

i) **Incorrect data**: While the risk of data integrity and reconciliation breaks is implicitly lower on DLT solutions, the risk of capturing incorrect data, which is then replicated amongst all participants, could prove challenging to resolve. AFME believes a private and permissioned design with adherence to a strong governance framework would embed the appropriate controls and cooperation amongst participants;

ii) **Interconnectedness risk**: The extent and propagation of a shock to actors may be exacerbated on a DLT environment due to the interconnectedness of nodes and potentially networks. AFME believes a private and permissioned design with adherence to a strong governance framework would embed the appropriate controls and cooperation amongst participants;

iii) **Cross border dispute resolution**: The risk of disputes due to losses or defaults may become more complex to solve for DLT solutions operating in different jurisdictions and in a virtualised environment. However, a DLT network operating on a private and permissioned design would allow to implement appropriate rules and controls in such events.

A governance framework for DLT would further support adoption and allowing for speed of processing whilst maintaining appropriate controls for safety and financial stability. A governance framework for DLT would have to solve for the following principles:

i) **Roles and responsibilities**: As seen by the 2016 Bank for International Settlements (BIS) report[8], a governance framework for DLT would have to consider the rights attached to each participant in the network such as (1) a system administrator acting as the gatekeeper controlling access to the system and providing certain specific services (2) the asset issuer permissioned to issue new assets (3) the proposer permissioned to propose updates to the ledger (4) the validator permissioned to confirm the validity of a state changes (5) the auditor permissioned to view the ledger but not make updates;

ii) **Vetting and approving participants**: Establish an accredited evaluation capability and an approval process that engages other network participants and relevant supervisors;

iii) **Monitoring compliance**: Establish an accredited capability for the ongoing review of network participant compliance against the governance framework and oversight of any agreed remediation actions;

iv) **Enforcing standards**: Establish a compliance review board comprising network participant appointees ensuring network participants maintain within the jurisdictional reach of the governance model as a condition of membership;

[8] 8 http://www.bis.org/cpmi/publ/d157.pdf

v) **Managing cross-border disputes**: Establish an independent arbitration panel and process to oversee disputes between network participants, and enshrine the legal enforceability of its decision within the rules of membership for each network participant;

vi) **Liability in the event of a cyber breach**: Although this may be applicable to cyber risks in general, DLT solutions will have to devised a mean to define, develop, and maintain a cyber resilience framework aimed at addressing current and emerging cyber threats, establish a cyber risk management capability, establish a cyber risk board amongst network participants;

vii) **Regulatory accountability**: Where relevant for certain use cases, engage relevant supervisors to agree on a framework through which regulators will ensure accountability of firms for the management of DLT functions.

Question 3:

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

While cyber threats and risk continues to grow, DLT networks will have to devise a means to become increasingly cyber resilient and proactive should the technology be implemented in financial markets. The use of messaging between participants and potentially smart contracts may increase vulnerability to cyber-attacks and contagion risks on a Distributed Ledger. However, DLT networks offer high levels of resilience to cyber threats due to the use of encryption, potentially active collaboration amongst participants (e.g. increasing detection capabilities), and data recovery capabilities due the distributed nature of data.

Achieving cyber resilience and security on a DLT network could be compared to the core principles of the National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity[9]. Two views of Cyber Risks on DLT are presented i) in the context of a public and permissionless design, ii) in the context of a private and permissioned design:

i) **Identify**: Identifying vulnerabilities may be more complex on a DLT network due to the potential complexity of IT systems (e.g. each node blending legacy and newer systems), the number of participating nodes (e.g. each a potential vulnerability), the interconnectedness of actors (e.g. financial market actors, market infrastructures, third party providers, regulators), based in different jurisdictions. However, identifying cyber vulnerabilities on a DLT network may be more easily achieved in a private and permissioned design where participants are bound to rules and controls ensuring consistent upgrade paths;

ii) **Protect**: The use of messaging between participants and potentially executable code (e.g. smart contracts) may increase vulnerability to cyber-attacks and breaches. Resilience via encryption and data partitions may more easily be achieved in a private network where effective coordination of participants is

[9] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

maintained. Furthermore, this could for the implementation of a system administrator, as part of the governance model, acting as the gatekeeper controlling access to the system and providing specific services;

iii) **Detect**: Identifying cyber threats may be more complex on a DLT network as explained under the above core principle "Identify". However, identifying an intruder on a DLT network may be more easily achieved in a private and permissioned design, where digital identities would support early detection efforts, and where participants are bound to collaborate more closely and coordinate efforts.

iv) **Respond**: An effective response in the event of a cyber breach may be more complex on a DLT network as explained under the above core principle "Identify". However, a private and permissioned design would allow the design and implement a cyber capability as part of its governance framework, defining liability in the event of a cyber breach. This capability would define, develop, and maintain a cyber resilience framework aimed at addressing current and emerging cyber threats, establish a cyber risk management capability, and establish a cyber risk board amongst network participants;

v) **Recover**: Data recovery may be more easily achieved in a DLT network due to the distributed nature of data. However, in the event of disputes this may become more complex if there is no participant coordination or central administration role. A private and permissioned design would allow for a governance framework where a system administrator and independent arbitration panel can monitor and solve disputes between network participants.

Question 4:

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

DLT solutions offer by design a high level of resilience due to the distributed nature of data, data encryption, data partitioning, a consensus mechanism to validate information, more integration points, and fewer single points of failure.

Resilience on a DLT network can be measured by its Recovery Point Objective (RPO). As defined by the Bank of England the RPO[10] is the maximum amount of data that may be lost when service is restored after an interruption. The RPO is expressed as a length of time before the failure. In a traditional centralised database system where data replication is asynchronous, there will always be a RPO greater than zero. This is due to the time gap between when transactions are recorded from the primary site to the back-up/recovery site. In the case of a DLT where consensus is distributed, the RPO would be reduced to zero in all nodes that have participated to the validation of the latest transaction. The reason is that validation of record updates in a DLT database occur among a set of nodes seeking consensus cooperatively; this

[10] http://www.bankofengland.co.uk/markets/Documents/paymentsystem/cp160916.pdf

model departs from the traditional master-slave replication of centralised database systems.

Resilience on a DLT network can also be measured by its Recovery Time Objective (RTO). As defined by the Bank of England the RTO[11] is the maximum time allowed for the recovery of a service following an interruption. The threshold which has been set for PFMI's by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) is 2 hours. On a DLT network, in case of a disruption, the validation of new transactions remains unaffected where the number of disrupted nodes is low and the surviving ones are sufficient to reach the necessary quorum. This means i) the greater the network of validating nodes the more resilient the network ii) consensus algorithms requiring a low quorum ensure better availability of the service. However, a balance is required as i) a high number of validating nodes diminishes throughput ii) a low quorum increases the possibility of tampering with the ledger by controlling a low number of nodes.

Further, DLT networks offer by design high levels of resilience in the case of a disaster recovery procedure. In the event of a node being taken off the network, the process for coming back to the network without significant data loss is more straightforward as other network participants hold a copy of the transaction ledger.

Resilience of a DLT network will depend on the resilience of each node which may be independently owned and managed by network participants.

AFME believes that to implement DLT on financial markets it must be ensured that each node is resilient, but also that the overall network architecture adopts technology, management and control standards that ensure the security of the network as a whole. Currently this may only be achieved in a private and restricted design with a rigorous governance framework.

a. DLT and distributed data

Question 5:

- *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?*

AFME is not responding to this question.

Question 6:

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

[11] http://www.bankofengland.co.uk/markets/Documents/paymentsystem/cp160916.pdf

DLT solutions may offer enhanced reporting and supervisory functions by allowing regulators to access directly transaction information as a node participant on the network. Therefore, it ought to be possible to eliminate regulatory reporting activities, placing control over data enquiry directly in the hands of regulators.

This would allow more timely and accurate information for regulatory reporting as data would be taken directly from the ledger without the need for a potential ETL (Extract Transform Load) interface.

However, AFME sees the following key challenges that need to be solved:

i) **Data sensitivity**: Data confidentiality will require careful data partitioning and encryption to ensure relevant participants access the right level of data. In addition, access to sensitive data may pose concerns in case of leakage or hacks. AFME believes this may only be effectively achieved on a private and permissioned design;

ii) **Technology Architecture:** Regulators will have to adapt their technological architecture to access data via the ledger and integrate this with their current processes. AFME believes that early engagement from regulators would allow for regulators to test and adapt their technology in a safe manner;

iii) **Global coordination:** Avoiding regulatory arbitrage through technology development, or implementation issues, will require a coordinated effort by regulators to minimise diverging regulatory requirements.

Question 7:

- *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?*

AFME believes that DLT solutions would not increase or introduce new financial crime risk, over-and-above those currently existing in the normal course of financial services activity. This is because any DLT network implementation within financial services will be private and permissioned.

Furthermore, to effectively mitigate financial crime on a DLT network, actors may have to consider means to enable digital identities. Identity is a key component for trust in financial transactions; this would require participants to identify themselves explicitly, pass network security checks and permission/entitlement checks to perform specific actions on the network. Transactions should be signed by the transacting party and validated by the counterparty. This would remove anonymity from transactions ultimately subject to adequate controls, for instance AML.

Further, AFME believes that DLT networks may render AML/KYC processes and mitigating financial crime more efficient:

i) **In theory mitigation of financial crime could be enhanced**, as transaction information, may be fully audited (e.g. immutability) and potentially accessible to any participating node;

ii) **The ledger could potentially support a broader range of data** linked to a fraudulent transaction, therefore supporting more effectively financial crime investigations and forensics (e.g. KYC, digital identities, data history);

iii) **Due to higher levels of cooperation** required amongst nodes to reach a consensus, financial crime may be more effectively mitigated.

However, key challenges may render financial crime mitigation more complex on DLT networks and will require actors to consider solving:

i) **Fragmentation** of DLT solutions may pose challenges on interoperability and render information access inefficient;

ii) **Geographical disparities** between financial crime regulatory regimes could increase regulatory arbitrage;

iii) **Data privacy regulatory requirements** such as the "right to be forgotten" under the EU General Data Protection Regulation 2016/679[12] (GDPR) may pose issues in the event of a criminal investigation where data is removed.

AFME believes that these challenges could be resolved under a private and permissioned design, while unlocking the benefits of mitigating more effectively financial crime.

b. Recordkeeping and auditability

Question 8:

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

AFME agrees with the use case presented by the FCA and supports the view outlined by SWIFT and Accenture in their 2016 report[13] on DLT:

i) **Efficient information propagation**: Latest data is updated and replicated in close to real time;

ii) **Full traceability of information**: New information is added to the ledger but not deleted creating an immutable chain of data where information is fully traceable;

iii) **Simplified reconciliation**: Mutualised information reduces reconciliation efforts;

iv) **Trusted disseminated system**: Data authenticity is completed by participants of the network rather than a central body;

v) **High resiliency**: The distributed nature of the information allows data to be recovered directly from any participant in case of local system failures.

The proof of concepts listed below[14] are currently being explored by the industry in the following areas which could benefit the context of asset management:

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[13] https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services

[14] p53 – 58, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

i) **Corporate records**: Using DLT for keeping track of securities ownership could reduce costs associated with the underwriting & tracking of ownership;

ii) **Corporate actions:** Using DLT to streamline process for managing corporate actions events (e.g. proxy voting, income distributions), removing duplicative processes and reconciliations between participants (e.g. issuing company, investors, intermediaries), to reduce administrative costs and manual processing requirements;

iii) **Post-trade**: Using DLT for clearing, settlement and asset servicing, to allow for near real-time settlement reducing counterparty risk, compliance and audit risks;

iv) **Asset tokenisation**: Using DLT so that bilateral trades potentially no longer require the services of an FMI, reducing intermediation costs;

v) **Contract execution**: using smart contracts on a DLT, to manage the lifecycle of financial products, to automate the execution tasks such as trade confirmations, cashflow verifications, payments, events management, and to reducing operational costs and risks;

vi) **Loan syndication**: using DLT as a common repository for data amongst multiple parties, the standard life cycle for syndicated loans emission could be significantly reduced by removing duplicative processes, currently taking several weeks on average;

vii) **Repo transactions**: Using DLT for record keeping of repo transactions and the tokenisation of collateral, to increase the transparency of collateral positions;

viii) **Short-term debt**: Using DLT to enhance the issue, trading, transferring, and redeeming of short-term debt by standardising and reducing transaction processing;

ix) **KYC/AML processes**: Using DLT to streamline KYC/AML processes by i) sharing client information to simplify on-boarding ii) increased transparency for transaction surveillance iii) one source of data for all transaction records, simplifying surveillance;

x) **Digital IDs**: Using DLT to store a combination of identity factors and records validated by trusted third parties, to improve KYC controls and financial inclusion;

xi) **Improving funding processes**: Using DLT to provide transparency on upcoming payments leading to efficient gains for cash management in treasury activities;

xii) **Alternative financing**: using DLT as a virtual, fully decentralised funding platform to provide funding to start-ups;

xiii) **Standardising securities processing and data records**: Using DLT to reduce Nostro breaks by having banks make payments based on ledger data.

Question 9:

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

AFME views the following examples of DLT as providing benefits to consumers:

i) **Financing**: Using DLT as a virtual, fully decentralized financing/lending platform to provide with more efficiency liquidity and financial products to consumers and start-ups;

ii) **Digital ID**s: Using DLT to store a combination of identity factors and records validated by trusted third parties, which may lead to significant benefits for consumers by decreasing the operational burden and costs required to interface with a broad range of digital platforms, systems, and marketplaces, and increasing financial inclusion;

iii) **On-boarding processes**: Using DLT to streamline client on-boarding processes by i) sharing client information to simplify on-boarding ii) increased transparency for transaction surveillance iii) use one source of data for all transaction records, simplifying surveillance.

However, key challenges on DLT networks may prevent the provision of benefits to consumers due to complexity, and will require actors to consider solving:

i) **Accessibility**: If access to consumer benefits are conditional on being able to access and use the technology;

ii) **Cross border transactions**: Fragmented regulations, standards and approaches to DLT solutions may limit the scope of consumer benefits;

iii) **Adequate consumer protection**: With the emergence of various DLT solutions in different jurisdictions, global cooperation and international involvement will be required to ensure adequate consumer protection is provided.

AFME believes that the full benefits of DLT will be provided through a private and permissioned design, ensuring that financial instruments may be provided with a high degree of control and suitability to SMEs and consumers, allowing for global and wide spread adoption across all actors of the eco-system.

c. Smart contracts

Question 10:

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

AFME notes the various definitions of smart contracts outlined in the FCA Discussion Paper (DP) including the one taken by the FCA, for the purpose of its DP, as “blockchain functionality to execute pre-determined commands without further human intervention”. However, it is important to clarify that smart contracts can be coded to require human intervention. So, whilst we can achieve greater and smarter efficiency, this does not necessarily result in lower control.

There is benefit in clarifying the potential amalgamation of two distinctive concepts included in smart contracts between “smart contract code” and “smart legal contracts”:

i) **Smart contract code**: Referring to the code stored and replicated on a blockchain, executed or run by a network of computers (usually the ones running the blockchain) or subset thereof, with capability for updating the ledger. This is no different than a tool used to transform products or services that may have, but do not require, existing legal frameworks. Using smart contracts according to those guidelines and constraints is comparable to using any other software-based tool for implementation and delivery;

ii) **Smart legal contracts**: Referring to that the application of technology towards augmenting or re-placing legal agreements, which is a specific use case of 'smart contract code'. To achieve "smart legal contracts" that are legally enforceable, developers would face extremely high technical challenges to represent complex legal syntax and its various cases as a computer code. The question also remains whether there is truly a market appetite for such transformation of legal agreements, as some contract clauses purposely rely on courts and human judgment for interpretation and dispute resolution e.g. determining liability under indemnity clauses.

AFME believes the above distinction is necessary too for the development efforts of smart contracts to achieve greater efficiency in specific use cases, and highlight that in certain situations human judgement may be preferable to automated executable code.

Based on the definition articulated previously smart contracts could offer the following benefits[15]:

i) **Speed**: Smart contracts use software to automate tasks that would have otherwise been manually processed, and could theoretically become instantaneous;

ii) **Accuracy**: Automated transactions are less prone to manual errors;

iii) **Execution**: Elimination of manipulation risk, non-performance, or errors, as execution is automatic rather than by an individual;

iv) **Number of intermediaries**: Smart contracts can reduce or eliminate reliance on third-party intermediaries that provide services such as escrow between counterparties;

v) **Lower cost**: Processes enabled by smart contracts require less human intervention and fewer intermediaries which can reduce costs;

vi) **New business or operating models**: New types of business models may emerge based on smart contracts by providing a low-cost means to ensure a transaction is reliably performed as agreed.

AFME identified the following use cases for smart contracts:

i) **Bond coupon payment**s: currently bond issuers maintain ownership records of bond holders, either directly or through a registrar and calculates the recipient, coupon payment amount and schedules transfers to specified accounts. Smart contracts embedded on a blockchain could automate the activities of i) maintaining ownership records of bond holders ii) identify

[15] https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html

bond holders and determining coupon payment iii) automate payment to specified accounts.

ii) **Insurance claim processing**: Currently insurance policies, once contracted, provide a specific payment to the party who files a claim in the event of a catastrophe. The claim is processed by the insurer to determine payment eligibility before a payment is made, which may take weeks or months. Smart contracts could become the de-facto insurance policy, where the external event could be registered or triggered by a valid data source (e.g. a hurricane occurs), thereby triggering the payment to the insured in near real-time.

iii) **Mutual fund subscriptio**n: Currently payments on fund subscriptions are a manual process whereby a transfer agent receives a request for payment (e.g. fund subscription order), calculates the payment amount based on the latest Net Asset Value (NAV) (e.g. received by the fund accountant), requests payment to the fund administrator and once approval has been received processes the payment to the investor. Smart contracts could support the current process by processing requests and payments of fund subscriptions requests received. A request for payment would trigger the smart contract to extract the NAV from a blockchain record and provide real-time payment to investors.

iv) **Central Securities Depository (CSD**): Currently CSD perform central notary, safekeeping and settlement services. DLT could optimise certain processes such as real-time settlement, automation of corporate action flows (using smart contracts or other means), optimising transfer agency processes, providing greater shareholder transparency.

v) **Trade clearing and settlement**: Currently this process provides approval workflows between counterparties, trade settlement amount calculations and automatic funds transfer. DLT and smart contracts could provide instant settlement but with the effect of constraining transaction netting. While netting may be possible on a DLT platform using smart contracts, netting as an activity may have limited benefits in a T0 environment, as DLT holds the potential to reshape the way post trade processes currently operate;

vi) **General product lifecycle management**: Smart contracts could be used to manage in a more efficient way manual or inefficient post-trade processes, such as trade confirmations, cashflow generation, cashflow verification, payments, or trade events management.

Question 11:

- *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?*

As observed by UK HM Treasury[16] digital currencies may provide benefits to financial markets by making payments faster, more convenient and more secure, which would potentially lower transaction costs and provide more business efficiency, in comparison to traditional payment means.

AFME believes that digital currencies provide similar benefits and risks to current systems, however noting that there are challenges specific to digital currencies, as articulated by the Federal Reserve[17]:

i) **Financial crime**: Digital currencies could be prime targets for theft, cyber-attacks, counterfeiting activities or money laundering activities. Advanced cryptography and security could reduce vulnerability to cyber-attacks but would make it easier to hide illegal activities. As well, anonymity often attached to digital currencies would exacerbate AML risks if these were not backed by a central bank, government, or a regulatory framework;

ii) **Data privacy**: To provide the appropriate means to combat cyber risks and financial crime activities, a record of digital currency issuance and individual transactions may be required to authenticate valid transactions. However, maintenance of such records could raise privacy concerns for personal and confidential data;

iii) **Instant payments and instant settlement**: While digital currencies may offer the ability to provide financial actors with instant payment or settlement, due to the current existing infrastructures and processes in place, this may not be a desired outcome and have indirect consequences on liquidity, funding, and collateral.

AFME believes many of the challenges posed by digital currencies could be resolved through appropriate implementation design (e.g. encryption, data partitioning, governance framework), testing and global cooperation. We support coordination across jurisdictions to avoid duplication and conflicting requirements.

AFME encourages current on-going efforts to explore the potential benefits of digital currencies such as the Bank of England[18] efforts under RSCoin[19] and the fundamental long-term research engaged on central bank-issued digital currency (CBDC)[20].

Question 12:

- *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?*

AFME believes that any deployment of DLT in financial services will benefit from a private and permissioned framework, rather than public and permissionless:

[16] https://www.gov.uk/government/news/bitcoin-litecoin-how-could-digital-currencies-revolutionise-the-way-we-pay

[17] https://www.federalreserve.gov/newsevents/speech/powell20170303a.htm

[18] http://www.bankofengland.co.uk/research/Pages/onebank/cbdc.aspx

[19] https://www.cryptocoinsnews.com/bank-of-englands-rscoin-a-hybrid-digital-currency-to-improve-global-trade/

[20] http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf

i) **Public and Permissionless**: Examples such as the Bitcoin and Ethereum blockchains, are open systems that have no restriction on participation. Participants function as nodes in the network, having the right to access the data in the ledger, add data to the ledger, and participate in the validation process. Public and permissionless DLT do not need a central counterparty or trusted participants. Instead, trust is replaced by the mathematical consensus algorithm built in the DLT;

ii) **Private and Permissioned**: Many of the potential areas of application and Proofs of Concept (PoC) that are being studied by the financial services industry are privately shared systems, between trusted parties that are permitted to access the system. The governing entities in the DLT (including shared ledgers) approve admission of new participants under certain predefined criteria, and specify nodes responsible for the verification process.

Although public and permissionless networks may enhance information transparency and improve network resilience through distributed data, AFME see the following inefficiencies that may be attached to these network types:

i) **Scalability**: Due to the number of potential participants, public and permissionless DLT networks are ultimately limited by transactions per second; currently this is not enough for real time settlement of securities and will continue to need significant increases in scalability and computational power;

ii) **Governance**: A public and permissionless DLT network must ensure the maintenance and sustainability of the network. If the verifying nodes quit the network and there are insufficient incentives to continue validating transactions, the remaining nodes may have little incentives to stay if the computational power required becomes relatively too expensive.

In addition, AFME believe that public and permissionless DLT networks present several risks for their implementation on financial markets, in comparison to private and permissioned networks:

i) **Regulatory and governance**: Public and permissionless networks would present financial stability risks, in the case of a network failure, as dispute resolution would be more difficult to achieve with virtualised entities based in different jurisdictions. Furthermore, regional regulatory differences could further exacerbate this issue such as financial requirements under Client Assets Sourcebook[21] (CASS), Dodd-Frank act[22], EU General Data Protection Regulation 2016/679[23] (GDPR) (e.g. "right to be forgotten"), Anti Money Laudering (AML), Anti Bribery and Corruption (ABC), Counter Terrorist Finance (CTF) or Tax compliance rules. It could also be more complex to manage digital identities in a public and permissionless network which

[21] https://www.fca.org.uk/firms/client-money-assets

[22] http://www.cftc.gov/LawRegulation/DoddFrankAct/index.htm

[23] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

could present increased financial crime risks (e.g. KYC/AML). Overall, co-ordination and control is more easily achieved in a private and permissioned network;

ii) **Privacy and security**: Public and permissonless networks could pose confidentiality and privacy issues regarding financial transactions. Anonymity is more difficult to achieve making these networks more vulnerable to confidentiality breaches. Private and persmissioned networks enable stricter control over data access or activity rights;

iii) **Counter-party and systemic risk**: Trust between parties is more difficult to achieve in a public and permissionless network, which would be exacerbated in the event of smart contract implementations, where actions are legally binding and parties are more difficult to identify;

iv) **Settlement risk**: Trading, clearing or settlement include a degree of counterparty risk which is the rationale behind Central Clearing Counterparties (CCP's) and Delivery Versus Payment (DVP) mechanisms as advocated by the International Organization of Securities Commissions (IOSCO). In public and private networks where counterparties are not easily identified, it could become more difficult for market participants to measure or assess their counterparty risk exposure;

v) **Technology risks**: Technology risk in a private and permissioned network, in terms of protocol upgrades, patching, software expansions, could be simpler to mitigate as participants are more easily identified facilitating coordination and communication.

Although Private and Permissioned DLT networks are easier to implement due to participants being known and identified trusted parties[24], public and permissionless networks are more likely to be open sourced and tested by a range of network participants. However, private and permissioned networks are not necessarily closed or entirely private as they could integrate aspects of open source. These hybrid networks, when carefully designed, implemented and tested, allow participants to take advantage of both networks, limiting the major risks outlined.

Question 13:

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

The risk to competition of a group of incumbents operating a closed network to the exclusion of others could create financial stability risks due to potential:

i) Reduced transparency or opacity of operations and transactions;
ii) Anti-competitive behaviours;
iii) Low levels of standards for consumer protection;
iv) Low levels of standards for security.

[24] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

However, the preferred choice of a private and permissioned network over a public and permissionless network for DLT implementation on financial markets, is for privacy and security concerns. AFME believes that appropriate protections can be designed and enforced via a well-defined governance framework. This transparent framework would align to regulatory requirements and regimes, whereby compliance could be monitored and enforced. Furthermore, in such a design regulators could have access to the network as a dedicated node.

2. DLT's COMPATIBILITY WITH THE EXISTING REGULATORY FRAMEWORK

a. Governance and technology resilience

Question 14:

- *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*

AFME believes that DLT adoption within the securities market could only be based around a private and permissioned design, with adherence to a rigorous governance framework. As articulated in "Answer 12" private and permissioned design are preferred due to their ability to generate trust amongst participants, having lower uncertainty in liability allocation and generally lower levels of vulnerability to Byzantine Fault tolerance (BFT)[25].

By design, any transaction inter-operating from a public and permissionless network to a private and permissioned network would have to adhere to the rules of controls (e.g. governance framework) of the private network, becoming de facto governed by the rules of the private network.

Examples of DLT implementations such as the Ethereum DAO hack in June 2016, have exposed the need to implement private designs where adequate controls can be enforced on participants. As articulated by the consulting firm Capco[26] operational risk on DLT have exposed the need to deliver a more complete framework, for post-trade securities operations and from a legal and regulatory perspective.

A private and permissioned design could be supported by a rigorous governance framework, achieving the balance needed to drive adoption, while establishing appropriate rules to allow for processing speed and maintaining appropriate controls for safety and financial stability:

i) **Roles and responsibilities**: As seen by the 2016 BIS report[27], a governance framework for DLT would have to consider the rights attached to each participant in the network such as (1) a system administrator acting as the gatekeeper controlling access to the system and providing certain specific

[25] http://pmg.csail.mit.edu/papers/osdi99.pdf

[26] https://www.capco.com/insights/capco-institute/~/media/Capco/uploads/articlefiles/file_0_1479206155.pdf

[27] http://www.bis.org/cpmi/publ/d157.pdf

services (2) the asset issuer permissioned to issue new assets (3) The proposer permissioned to propose updates to the ledger (4) The validator permissioned to confirm the validity of a state changes (5) The auditor permissioned to view the ledger but not make updates;

ii) **Vetting and approving participants**: Establish an accredited evaluation capability and an approval process that engages other network participants and relevant supervisors;

iii) **Monitoring compliance**: Establish an accredited capability for the ongoing review of network participant compliance against the governance framework and oversight of any agreed remediation actions;

iv) **Enforcing standards:** Establish a compliance review board comprising network participant appointees ensuring network participants maintain within the jurisdictional reach of the governance model as a condition of membershi;

v) **Managing cross-border disputes**: Establish an independent arbitration panel and process to oversee disputes between network participants, and enshrine the legal enforceability of its decision within the rules of membership for each network participant;

vi) **Liability in the event of a cyber breach**: Define, develop, and maintain a cyber resilience framework aimed at addressing current and emerging cyber threats, establish a cyber risk management capability, establish a cyber risk board amongst network participants;

vii) **Regulatory accountability**: Where relevant for certain use cases, engage relevant supervisors to agree on a framework through which regulators will ensure accountability of firms for the management of DLT functions.

b. Digital asset trading

Question 15:

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

AFME agrees with the use cases presented by the FCA in its DP but several additional factors should also be considered:

i) **Model A** is a DLT used for internal recordkeeping purposes by a single firm. For large firms with multiple subsidiaries and multiple business requirements, such as intra-firm transfer pricing models, this model may provide significant benefits for deployment;

ii) **Model B** is a DLT-enabled transaction processing and settlement platform. AFME believes this example is a good illustration of a process enhanced by DLT as it provides a platform to market participants that enhances transaction traceability, confirmations/settlements functionality, final settlement at “fiat” level or at a central clearinghouse, facilitating in fine settlement finality;

iii) **Model C** involves a third-party digital currency to settle payments related to the purchase and servicing of assets. Although such a model could be technically feasible today, legal and regulatory endorsement to replace or integrate with the role of fiat currencies in existing financial infrastructures requires more support than the proofs of concepts currently being by the industry[28].

Overall, AFME believes that factors of success of DLT implementations in financial markets should be based on the following principles:

i) **Private and permissioned networks** over public and permissionless would enable trust among participants;
ii) **Endorsement of a rigorous governance framework** would drive standards and controls reinforcing inter-operability and security;
iii) **International engagement of the financial services eco-system** would enable scalability and assimilation of a broader range of a product life cycle;
iv) **Continuous monitoring of how DLT is transforming business models** to accommodate the regulatory framework to potential role changes (e.g. CCP's).

The following proof of concepts[29] are currently being explored by the industry in the following areas:

i) **Corporate records**: Using DLT for keeping track of securities ownership could reduce costs associated with the underwriting & tracking of ownership;
ii) **Corporate actions**: Using DLT to remove duplicative processes and reconciliations between participants (e.g, issuing company, investors, intermediaries);
iii) **Post-trading**: Using DLT for clearing, settlement and asset servicing, could allow for near real-time settlement reducing counterparty risk, compliance and audit risks;
iv) **Asset tokenisation**: Using DLT so that bilateral trades potentially no longer require the services of an FMI, reducing intermediation costs;
v) **Contract execution**: Using smart contracts on a DLT, to manage the lifecycle of financial products, would automate the execution tasks such as trade confirmations, cashflow verifications, payments, events management, reducing operational costs and risks;
vi) **Loan syndication**: Using DLT as a common repository for data amongst multiple parties, the standard life cycle for syndicated loans emission could be significantly reduced by removing duplicative processes, currently taking weeks on average;
vii) **Repo transactions**: Using DLT for record keeping of repo transactions and the tokenization of collateral, would increase the transparency of collateral positions;
viii) **Short-term debt**: Using DLT to enhance the issue, trading, transferring and redeeming of short-term debt by standardizing and reducing transaction processing;

[28] https://www.finextra.com/newsarticle/29345/ubs-wins-big-bank-backing-for-utility-settlement-coin-concept
[29] p53 – 58, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

ix) **KYC/AML processes**: Using DLT to streamline KYC/AML processes by i) sharing client information to simplify on-boarding ii) increased transparency for transaction surveillance iii) one source of data for all transaction records, simplifying surveillance;

x) **Digital IDs**: Using DLT to store a combination of identity factors and records validated by trusted third parties, could improve KYC controls and financial inclusion;

xi) **Improving funding processes**: Using DLT to provide transparency on upcoming payments leading to efficient gains for cash management in treasury activities;

xii) **Alternative financing**: Using DLT as a virtual, fully decentralized funding platform to provide funding to start-ups;

xiii) **Standardising securities processing and data records**: Using DLT to reduce Nostro breaks by having banks make payments based on ledger data;

Question 16:

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

AFME recognizes that one of the key legal and regulatory challenges will be to define whether ICOs should be treated as currency, securities, or commodities. As the appropriate regulatory treatment for these may greatly vary, AFME believes approach to ICOs should globally harmonised across jurisdictions, treated as an innovation and on a case-by-case basis.

c. Collateral management

Question 17:

- *Are there other parts of regulation where DLT might offer a new market convention?*

AFME believes further clarity is required in relation to the question posed and its relation to collateral management. However, the following general approach should be taken in cases where DLT offers new market conventions:

i) **Testing**: In the event of DLT implementations posing challenges within regulations, policymakers should take a pragmatic approach. Regulators should first contemplate and test how the technology is impacting financial stability and consumer protection, as the current regulatory framework did not contemplate for a technology such as DLT;

ii) **Regulate the application of DLT, rather than the technology**: The potential use cases for DLT are 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, AFME believes the technology itself should not be regulated. Any regulatory action should be determined on a case-by-case basis, rather than the sole determining factor being the use of DLT.