4th floor, Ropemaker Place
25 Ropemaker Street
London EC2Y 9LY
United Kingdom

+44 20 7260 2000 Phone
+44 20 7260 2001 Fax

ihsmarkit.com

FCA
25 The North Colonnade
Canary Wharf
London E14 5HS

Submitted via email dp17-03@fca.org.uk

London, July 17th 2017

Discussion paper on Distributed Ledger Technology

Dear Sirs,

IHS Markit is pleased to submit the following comments to the Financial Conduct Authority (FCA) in response to its Discussion Paper (DP) on Distributed Ledger Technology (DLT).

IHS Markit[1] (Nasdaq: INFO) is a world leader in critical information, analytics and solutions for the major industries and markets that drive economies worldwide. The company delivers next-generation information, analytics and solutions to customers in business, finance and government, improving their operational efficiency and providing deep insights that lead to well-informed, confident decisions. IHS Markit has more than 50,000 key business and government customers, including 80 percent of the Fortune Global 500 and the world's leading financial institutions. Headquartered in London, IHS Markit is committed to sustainable, profitable growth.

Comments

DLT has captured the imagination of financial markets, policymakers and regulators. The successful implementation of DLT in the Bitcoin protocol has led financial market participants to consider potential use cases in the securities and derivatives markets. A number of firms are investing significant resources in potential solutions;

[1] See www.ihsmarkit.com for more details

participating in Proofs of Concept and successfully experimenting with applications of DLT.

IHS Markit has been at the forefront of these efforts in wholesale financial services. We are members of the US Chamber of Digital Commerce, are represented on the CFTC Technology Advisory Committee. IHS Markit firmly believes in the potential of DLT and has invested significant resources in developing solutions around Entity Data, Smart Contracts and Cash Transfer Protocols for Settlement. We are currently creating a distributed financial network built on DLT infrastructure, offering a series of transaction management and asset servicing applications for firms to manage trade lifecycles more efficiently and with less operational risk, including:

i) a token-based protocol that can be converted to fiat currency, facilitating collateral management and cash movement for settlement and custody of assets;
ii) standardised, smart contracts that automate workflow for trade confirmation, clearing and regulatory reporting as well as post-trade lifecycle events; and
iii) identity management that incorporates KYC requirements and OFAC / AML validation, both for entities and individuals.

IHS Markit believes that DLT will transform global securities markets. Back office processes such as confirmation/affirmation and reporting could benefit from the efficiencies of DLT in the next 2-3 years. Applications in capital market operations such as issuance and trading are likely to take longer since these require fundamental change in securities markets and legal frameworks.

Widespread adoption of DLT in capital markets is predicated on a clear definition of digital assets. Regulators should create a legal framework for digital assets that will help market participants create DLT networks. The successful application of DLT in capital markets will also require cross-border coordination between industry participants and regulators.

We welcome the interest of the FCA and this DP and are happy to provide our comments on the questions below. We stand ready to discuss these comments or our projects and experience.

Questions

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?

The FCA has a number of initiatives to promote innovation and the take up of FinTech and RegTech solutions, most notably through Project Innovate. The issues around DLT and outsourcing appear very similar to those around outsourcing and innovation generally. When adopting RegTech services from a third party under outsourcing

arrangements, firms should demonstrate that adequate risk-based analysis has been conducted. If the outsourced service is classed as material, there are significant additional compliance burdens and costs, something which can affect the viability of potential solutions and be a drag on innovation and the take up of DLT based solutions. We believe that it is important that services are only classified as "material outsourcing" when this is fully justified.

To avoid stifling innovation the FCA should:

- Define clear, objective criteria to determine whether the use of a third party service represents "material outsourcing" and ensure clear and proportionate requirements for providers under material outsourcing;
- Facilitate compliance for material outsourcing service providers to "comply once" rather than having to demonstrate compliance separately to numerous clients for the same service. This could potentially be supported by, for example, the use of a registry.

When adopting DLT, a firm's risk based assessment should include a review of that DLT network's operational standards and performance. Specifically when adopting public, permissionless DLT networks, it will be important to ensure that due diligence questionnaires focus on network security protocols and data encryption standards.

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?

The key operational risk in the implementation of DLT is around the interoperability of that system into existing workflows. This means that firms must ensure that DLT-based services are compatible (or otherwise interoperable) with existing systems and processes that are not being replaced. Other operational issues include identity management and network "ownership".

When implementing DLT systems, both hardware infrastructure and enterprise software are required to operate a node effectively and can be delivered by a cloud-based technology solution. With cloud-hosted infrastructure, firms like Amazon Web Services, have mitigated operational risks by working with Financial Services industry participants and service providers (such as IHS Markit) to understand data security, data transfer, and data governance requirements.

We envisage firms migrating to micro-service based architecture. This will offer better control over deploying updates across cloud-hosted systems on a firm-by-firm basis, while maintaining connectivity to the broader network – including with firms that are not on the distributed network. Cloud-based, micro-services architecture also reduces operational risks in implementing DLT systems by isolating issues that are node or firm specific and reducing potential risks from affecting multiple firms.

On a system wide basis, some firms seem to be concerned about ideas that "code" will be "interpreted incorrectly" and somehow allowed to run amok. We do not believe such a scenario is possible. Too often, firms take into account exceptional cases of systemic problems in digital currency without understanding the proper context.

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

The best way for DLT networks to protect themselves against network security penetration is to encourage the network's use and growth. The larger a distributed network becomes, the less burden each individual user has to bear in order to uphold the network's security.

DLT networks, by their nature, minimise the incentive of an attack and maximise the costs for the attacker. Instead of simply attacking the single node that contains sensitive data, an attacker must amass a majority stake of processing power in a distributed network in order to gain any control. The larger the network, the higher such costs will be.

When considering public, permissionless networks, high standards of network security are built in. However, the current state of security on the edges must be improved. As far as we know, security concerns in public networks have never resulted from flaws in the network protocol, but rather from lapses with end-user security. This can be addressed by security parameters that are updated at high frequency with short time intervals, along with multi-factor authentication of network participants when attempting to access the network.

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

When it comes to DLT, it probably helps to think about it providing a resiliency trade off. When a network maintains a replicated copy of information across every peer, the likelihood of an attempted attack on the system is minimal, as is the likelihood of the success of such an attack (see also our answer to question 3). However, this comes at considerable cost. Every single network participant has a copy of every single data point. Therefore, at an aggregate level, the costs of this kind of framework can potentially far exceed those associated with hub-and-spoke network setups.

Furthermore, DLT requires fail-over to ensure a participant node on the network is not compromised and removed from the network. If the participant node is removed, consensus fails and this could bring down the network. However, fail-over to a previous implementation (in effect akin to a system restore) may facilitate continued operations, and allow for the investigation of the failure to run in parallel.

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

DLT offers enormous potential to reduce costs and increase the effectiveness of regulatory reporting as it can benefit from shared, replicated ledgers used across specific networks. We are unaware of regulatory reporting use cases that have already been live-tested, but they have certainly been considered.

To make these systems effective, there must be differentiation between trade reporting (also known as post-trade transparency) and transaction (or regulatory) reporting. Trade reporting is public information for market consumption. It can have a wide audience which can be shared in real time among the participants of a DLT network. However, regulatory reporting is usually confidential data sent only to the regulator; it may be market sensitive (for example, illiquid transactions, delivery locations) or confidential entity or personnel data that cannot be shared more broadly due to banking and privacy laws. It is therefore important that private data required for reporting are not divulged to the broader network of participants. This further increases the need for effective network permissioning to differentiate it from data that can be made publicly available to network participants.

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?

DLT potentially provides a tamper-proof dataset of asset movement across a network and so has great potential to mitigate risks around financial crime. To be effective, distributed networks will require effective governance frameworks and network security.

Governance structures must ensure that only authorised participants can make use of the network and that the network is not misused. The governance structure should include strong "know your customer" processes and have adequate transactional audit capabilities to minimise the risk of financial crime.

DLT shows obvious potential in mitigating financial crime risks related to money laundering. Although DLT will not stop money laundering, it will provide an irrevocable trail for money and asset movements. This will make it much easier and quicker to identify money laundering patterns and tactics with less specialised intelligence compared to the current situation.

Furthermore, we would encourage authorities to ensure that definitions and enforcement processes around financial crimes are workable in DLT environments.

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

Asset management workflow can be simplified and streamlined if the assets in question are digitised and managed on DLT. The key to this solution lies in the ability of DLT to provide a single version of a known "truth" to multiple users across a network. The process of reconciling versions of such a "truth" across parties is time consuming and expensive and typically outsourced to third parties. DLT can commoditise this third party role and save costs for users.

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

It is important to remember that ultimately DLT, very much like the internet, will be at the heart of the out of sight mechanisms that will enable consumers to enjoy the benefits and access new services DLT might help bring about. The benefits of shared networks should lower the cost of financial services and offer access to new liquidity sources for providers of credit and potential customers.

Natively digital assets owned by consumers offer direct and tangible benefits through lower transaction costs in asset transfers. Where there are several wire transfers associated to settling transactions, the ability to do this with digital assets will allow for operational risk reduction and cost efficiencies, benefits that will flow to consumers.

Additionally, consumers will enjoy direct and tangible benefits from DLT with respect to reduced fraud from the existence of a singular record of the current ownership of an asset on DLT. With a shared version of the "truth" and an associated audit trail, fraud becomes much more difficult to commit. Consumers should benefit directly from the additional trust and lower risk of fraud offered on a distributed network that provides consensus to asset ownership.

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

Smart contracts have existed in imperfect form in financial services for decades. The term "smart contracts" should simply refer to the financial services industry's ability to automatically keep complex multiparty agreements current by, for example, automatically updating data fields due to contract intrinsic events. Systems have already come a long way from paper certificates through to the electronification of agreements, correspondence and asset servicing. How distributed ledgers will shape the next phase of this automation remains to be seen.

Therefore, we would respectfully disagree with the FCA's definition of smart contract as "blockchain functionality to execute pre-determined commands without further human intervention".[2] This does not acknowledge existing, non-blockchain/DLT-related smart contracts that are ubiquitous in financial and commodity markets. We would suggest a definition of "smart contract" that was less tied to blockchain technology, such as "automated functionality to execute pre-determined updates without human intervention."

As a leading processing platform for derivatives and loans, our platform is already used to facilitate the creation of legally binding smart contracts. These smart contracts are, in turn, the basis of automated and manual processes, leading to clearing and settlement, regulatory reporting, and other lifecycle events. DLT use cases that have been live tested include the confirmation of credit derivatives and equity swaps by way of smart contracts. With a number of test cases demonstrating the value of using DLT, by both increasing operational efficiency and reducing operational risk, it is clear participants in financial services will seek to continue adopting smart contracts, albeit they will not do this all at the same time.

What DLT enables is greater automation of financial contract workflows through the use of processes that ensure accuracy and validation. For that reason, IHS Markit has invested heavily in DLT applications. What remains to be determined is the level of logic that will be on a public DLT against what will be maintained off the DLT infrastructure (or kept private). This may vary on a firm-to-firm basis, and requires an understanding of the level of standardisation that exists with firms' internal processes.

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?

Digital currencies change the risk behaviour of assets through digitisation. That assets can be fully digitised and transferred based on a set of prescribed rules is a step change in the movement of assets across the global financial system. This brings with it two key benefits: a decrease in the barriers to entry for financial services; and an increase in financial asset diversity. Cheaper financial services come as the costs of moving digital goods across the internet remain extremely low in comparison to physical cash and assets. The costs associated with moving paper money and items like precious metals are non-existent in the digital currency world. Improved financial asset diversity comes about as digital currencies' values are determined in unique ways, typically left to

[2] DP 3.34

market forces. This combines money like behaviour with assets whose intrinsic values are determined by the market.

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?

The development of private distributed ledgers could end up being a case of reinventing the wheel. Public distributed ledgers provide a commoditised alternative to bespoke processing mechanisms in financial markets and are successful precisely because they are not specialised. Their availability and robust architecture leads to scale, so long as their added value is proven for end users.

The discussion around private distributed ledgers seems analogous with the development of the internet. Attempts were made to build private walled gardens of contained internet access. Although these efforts were not without merit, they simply could not compete with a public alternative – why build private networks when a public one serves 99% of your needs? We believe that the benefits of public networks are similar to those of the public internet and, therefore, expect development to follow along similar lines.

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?

There are multiple points of responsibility for any use of a public network and these responsibilities are dependent on what is being sent across the network. For example: Who is responsible for maintaining equity value of a company? Who is responsible for internet reliability? Who is responsible for understanding what one buys and sells in financial networks? Who is responsible for legal dispute resolution? Who is responsible for maintaining custody of assets?

These are all known issues that could be applicable in many different circumstances. But the questions must be asked and answered in a world of digital assets maintained on a distributed network.

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

We do not expect major trading activity to take place on DLT (for example, due to latency), therefore this is not an area we would expect to greatly benefit from DLT networks. However, the custody transfer of value by way of digital assets, including securities issuance, would. Firms are therefore likely to see securities issuance as a big benefit from DLT.

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

The industry should define the characteristics of a "coin" to provide guidance on how to move forward. "Coins" can provide the liquid characteristics of cash with governance structures of equity. Consideration of coins' capacity as a unit of value and equity storage vehicle should guide any regulation.

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

One regulatory theme could be that of digital currency tokens and their interoperation with physical currency. This is a critical component of any DLT network used for payment or that results in payment. A reasonable regulatory approach should be developed for these types of DLT applications, including clarity on what payment related activities require authorisation or are subject to regulatory requirements (such as capital and liquidity requirements, AML, KYC, operational risk management requirements, fiduciary standards, etc). We believe the FCA could provide valuable assistance in forming a regulatory framework around DLT-related payments activity, including the use of virtual tokens used to process cash on a distributed ledger. In any clarification, we would recommend the FCA adopt an activities-based approach to regulation, in line with its traditional philosophy.

****

We hope that our above comments are helpful. We would be more than happy to elaborate or further discuss any of the points addressed above in more detail. If you have any questions, please do not hesitate to contact us.

Yours sincerely,

David Cook

Head of European Regulatory Affairs
IHS Markit
david.cook@ihsmarkit.com