ISSA

Distributed Ledger Technology

Principles for Industry-Wide Acceptance

Version 1.0 Report

June 2018

Abstract

The ISSA Symposium held in May 2016 devoted substantial time to transformative technologies and in particular to Distributed Ledger Technology (DLT). Intensive breakout group discussions at the Symposium highlighted a number of needs to be addressed by ISSA. The ISSA DLT working group was tasked to delineate the principles by which distributed ledger networks could operate.

This report explores and highlights the principles that should be followed by the industry players in the governance, information security and regulatory aspects of implementing this new technology. The existing ISSA principles embodied in its many white papers are also looked at and are analyzed as a proxy for changes DLT may cause in securities services practices in the near future. The report concentrates on the application of DLT to conventional asset classes serviced by custodian banks and CSDs / ICSDs, such as equities, bonds, funds and derivatives. The topic of "Crypto Assets" in its wider sense will be explored further in future ISSA publications.

Target Audience

This report should be of interest to securities services professionals who are considering the role this new technology may have in their own institutions. It also provides valuable background information for FinTech companies, industry associations and regulators.

Acknowledgements

This report is the result of efforts by a team of experts drawn from ISSA Operating Committee members and other ISSA participating member firms. All participants supplied valuable market information. The names of participating firms and the individual contributors are listed in Appendix 4. The ISSA Executive Board wishes to thank all supporters for their contributions as well as their firms having enabled their participation.

Disclaimer

It is ISSA's intention that this report should be updated periodically. This document does not represent professional or legal advice and will be subject to changes in regulation, interpretation or practice.

None of the products, services, practices or standards referenced or set out in this report are intended to be prescriptive for market participants. Therefore they should not be viewed as express or implied required market practice. Instead they are meant to be informative reference points which may help market participants manage the challenges in today's securities services environment.

Neither ISSA nor the members of ISSA's Working Group listed in Appendix 4 of this report warrant the accuracy or completeness of the information or analysis contained in this report.

International Securities Services Association ISSA
c/o UBS Switzerland AG
EUR1 – EG2230, P.O. Box
CH-8098 Zurich, Switzerland
Contact +41 (0)44 239 91 94
issa@issanet.org

Table of Contents

1 Executive Summary

The key points summarized below have been outlined in this report. General aspects are followed by distinct sections on governance and information security. A large body of work containing the review of the potential impact on the currently published ISSA Principles and a roundup of Regulatory Initiatives around the globe are in the Appendix section.

1.1. General

- Distributed Ledger Technology (DLT) has received widespread attention by securities servicing professionals due to the potential transformation it could bring to post-trade processing.
- This paper should be of interest to securities services professionals who are considering the role this new technology may have in their own institutions.
- DLT has introduced a new model for securely shared data, allowing financial firms to share a database of financial transactions instead of each firm maintaining their own and then reconciling differences. DLT also brings additional features such as blockchain, which is a method of recording transactions with built-in immutability and consensus to decentralize ledger updates.
- It should be understood that DLT is still at an embryonic stage of development and as such future developments may lead to revisions in the content of this document.
- The ISSA DLT paper examines the enabling capacity of this technology, the strong potential for new business models emerging and significant increases in operating efficiencies. At the same time, it takes the perspective that a DLT solution should offer equivalence or improvements to current ways of operating – in terms of transparency, security, data integrity, privacy, stability, governance and regulatory compliance.
- Financial services models operate in highly regulated and permissioned models today, and hence the paper assumes this will continue with DLT, rather than any departure to a permission-less DLT environment similar to the one Bitcoin is operated on.
- Entities should carefully consider the need for a consensus algorithm if there is a natural entity that already acts as the authority for a ledger.
- It is unlikely that the industry will develop a single ledger with one ruling governance body, the paper therefore anticipates multiple ledger models across the financial services ecosystem, driving a need for uniform business standards and high levels of technical interoperability between ledgers and with legacy environments.

1.2. Governance

- DLT changes the individually owned and governed silos of data responsibility into a shared, distributed database with shared ownership. As a result, the use of DLT places a heightened importance on the governance models by establishing clear lines of responsibility, which must be prioritized for any DLT model.
- Although existing securities financial markets are tightly regulated with permissioned models that restrict information access, it is likely that DLT models will drive the evolution of more integrated approaches – accentuating the importance of very robust membership and access eligibility controls.
- Accountability of all aspects of the DLT governance should be explicitly specified as part of the services designed, including oversight, monitoring and intervention

protocols, vendor and vendor software management, accountability for network membership and participant identity proof controls.

- A broad set of conduct rules should also be defined by the governing body to include recourse mechanisms, dealing with fraud and hacking, and use of smart contracts and other shared algorithms and automation codes.
- Transaction finality is a key constituent of existing models, and DLT systems must be able to define finality in compliance with existing regulations and laws. The validation of legal record basis and the consideration whether selective records carry higher standing in the event of disputes on legal records should be carefully assessed.
- A framework for DLT risk assessments should be considered including the assessment of transaction risk, concentration risk, credit and insolvency risk, business and operational risk, cyber risk and regulatory/compliance risk.
- Increased data access by regulators should also be considered, balancing the benefits of ease of access including immediate transparency and reduced costs of regulatory reporting with necessary control issues including increased public sector investment in information systems that are derived from an unabridged data access in a single node.
- Sources of data should be defined and assessed by governing bodies, with clear controls on parties authorized to introduce data to the DLT network.
- Data privacy and GDPR (General Data Protection Regulation) themes should be considered, taking into account respective country laws and restrictions on data flows across borders.
- Not all data held will have equal sensitivity, and it is important that this is carefully assessed and that the potential impact of breaches in data protection and privacy are assessed.
- The post-trade securities markets are highly interconnected, therefore it is critical that interoperability between market participants, platforms and related outside infrastructures is considered from a control and governance perspective.
- Technical interoperability gives weight to the importance of standards and interledger protocols. There are clear benefits to the industry for collaboration of DLT vendors to common standards that enhance interoperability. It also needs to be explored whether existing financial standards can be leveraged and extended.
- Standards scope should include the definition of business concepts and processes, common definitions and templates for smart contracts, and common mechanisms for legal and smart contracts.

1.3. Information Security

- There is a significant change of approach that DLT models have over existing segregated ledger models that leverage entity distinct versions of truth, extensive bilateral reconciliation models and entity controlled data access and protection.
- Financial services models are highly permissioned with a strong focus on confidentiality. Systems today place a clear emphasis on confidentiality over integrity. DLT models should be developed to support that perspective.
- There are a number of existing and emerging options for configuring DLT models for financial services that add complexity to the selection of the right model and approach. Diverse DLT models and implementations will increase risks and will require enhanced security models to ensure integrity is maintained across interoperability boundaries.

Data Security and Confidentiality

- Data confidentiality models need to consider how data access is restricted to relevant counterparts and how to leverage strong encryption models and on-chain and off-chain data models to achieve these goals.
- Whether sensitive data is stored on-chain or off-chain has major implications for information security and needs to be diligently assessed. Segregating data onto separate networks for the purposes of confidentiality can introduce similar issues with data silos as exist today.
- The data confidentiality model should be performant, allow for continuous execution of processes and not compromise the integrity of the overall network state.
- On-chain data confidentiality options include leveraging disjoint network models to reduce participant access and a variety of data encryption techniques including zero knowledge proof models.
- Encryption for maintaining fully shared sensitive data can be subject to graph analysis to reveal sensitive information including activity patterns and volumes, and this can increase the attack surface for malicious actors.
- Zero-knowledge proofs are an interesting but insufficiently tested cryptographic technique that could potentially introduce highly complex security vulnerabilities. This needs careful assessment as the concept evolves.
- Off-chain data confidentiality options restrict the amount of data held on the chain, limiting data access if unauthorized access occurs, but there are challenges to managing split data models including transaction uniqueness controls and data security.
- Uniqueness services can support the avoidance of transaction duplication and one-way cryptographic hashes provide a model that is stronger than basic encryption and that cannot be reverted.
- There is a convergence of platform designs towards the use of the insertion of fingerprints onto a blockchain with private data being shared point to point.

Data Integrity

- Data integrity models need to address the trade-off between confidentiality and integrity as network priorities, and this impacts the design and options for integrity models covering data integrity synchronization.
- Requiring all parties to sign transactions at the point of time that they are committed introduces new security and operational risks.
- If a consensus algorithm is required, there are many trade-offs to consider between approaches in this young but rapidly evolving field, including different consensus algorithm options that deal with consensus failures in different ways.
- Post-commit validation approaches can also be suitable for financial services, but perhaps only in circumstances in which there is already an authoritative party to leverage. These approaches assign master privileges to a single entity to maintain the ledger, while allowing participants options to independently verify transactions.
- Regardless of data integrity synchronization models, distributed ledgers are most able to maintain integrity when assets are on-ledger in purely digital form. Other risks prevail where primary asset custody is outside the DLT model, but then tokenized or reflected on the ledger.

Smart Contracts

- The integrity of the ledger cannot be relied upon if the smart contracts themselves are compromised, so these contracts require careful oversight, validation and control.
- There is a growing list of smart contract languages supporting different DLT platforms. Transactions in the financial services industry will likely require the need to span multiple ledgers across different DLT platforms. Standards and interoperability protocols for smart contracts across languages and platforms is a necessary requirement to support real-world transactions.
- The design of the language employed for smart contacts contains numerous nuanced design decisions that have major security implications for multi-party financial workflows. General purpose programming languages may not be well suited to this new domain.

Digital Identity Keys and Disaster Recovery

- Identity keys are a critical control area that should be reviewed carefully. Access control depends on the quality and security of digital identities, and these keys must be protected from outside exposure.
- Identity systems should support the delegation of responsibilities to third parties in order to match the market structures that exist today, including for example delegation of actions to custodians.
- DLT is not a replacement for current disaster recovery approaches but does provide some additional properties that could enhance recovery options.

2 Introduction

Since the arrival of Bitcoin, first described in the 2008 whitepaper by Satoshi Nakamoto, the financial industry has been captivated by the promise of the blockchain technology that it was based on. Blockchain or more generally the Distributed Ledger Technology (DLT) has been hailed as anything from a disruptive force that will eliminate all friction between capital raisers and investors and thus sweep away the industry's business models to the panacea that will solve forever the inefficiencies and asymmetries of industry automation. As the initial excitement surrounding the technology subsides and credible DLT implementations emerge, it becomes clear that neither outcome is likely to materialize in the short-term. This is not to diminish the transformational potential of the technology, rather to acknowledge that the financial industry is a complex, interconnected and highly-regulated system, that is tied closely to the functioning of the global economy with high bars for risk management and investor protection. With so many interests represented, this creates obstacles to change that are difficult to overcome, no matter what the ultimate benefits.

This paper, in sync with the ISSA mission, focuses on the global securities services industry (the pure payments side apart from delivery of securities versus payment is not part of this paper). In the financial industry, the identity of actors and clarity around the role and responsibilities of each is fundamental. This has led to the emergence of *permissioned* DLT implementations, which assume the existence of known participants and an authority that grants permission to participate. In this paper we focus on permissioned systems only (compared to a non-permissioned DLT environment such as the one underlying Bitcoin etc.). The paper explores and highlights in more detail the principles and developments that should be followed by the industry players in the governance, information security and regulatory aspects of implementing this new technology. The paper concentrates on the application of DLT to conventional asset classes serviced by custodian banks and CSDs/ICSDs: equities, bonds, funds and derivatives. The existing ISSA principles embodied in its many white papers are also looked at and are analyzed as a proxy for changes DLT may cause in securities services practices in the near future.

There is currently an explosion of interest and activity around initial coin offerings (ICOs), new crypto-assets and tokens, and servicing them as an emerging new asset class, but this remains a rapidly changing and volatile area. ISSA believes it is premature to attempt to provide authoritative guidance to the industry on these developments.

The paper consists of 4 main sections, covering governance, information security, implications of DLT for existing ISSA principles and regulation across the globe.

The **Governance** section sets out the fundamentals of permissioned DLT implementation and describes the variety of different deployment models. It goes on to discuss the governance implications, the role of DLT system operators, market participants and regulators, both when the platform is operating normally and when something goes wrong. It also tackles one of the key concerns for the implementation of DLT in a complex and interconnected value-chain: how to ensure interoperability between applications built with the new technology and existing business processes based on legacy technologies deeply embedded in thousands of financial institutions and utilized by their millions of customers.

Information Security discusses the special data security and privacy benefits and challenges of DLT, looking at the different ways in which permissioned DLT solutions implement data sharing and the implications in terms of data integrity, resilience and data privacy.

This section examines how the confidentiality model employed not only has implications for the security of sensitive data but also for the overall integrity of the single shared source of truth, concluding that the choice of confidentiality model can recreate the same silos that exist today. The use of encryption or zero-knowledge proofs are currently not suitable and there is a convergence of platform designs towards point to point sharing of data with only fingerprints of that being replicated across the networks. This section then looks at how the integrity of the network is maintained and the risks involved in requiring transactions to be signed at the time that they are committed, compared with them being verified independently after the fact. It also looks at the risks introduced with the use of consensus algorithms and whether they are even required in financial markets with permissioned networks and existing central infrastructures. It then covers an area that has had relatively little discussion, the safety and security of smart contract languages and whether the adoption of general purpose programming languages is suitable for a new multi-party domain or whether the new domain requires a purpose built language. Lastly it explores the implications of DLT for digital identity and disaster recovery, concluding with several key considerations when choosing a DLT platform.

In the Appendix existing **ISSA Principles** are reviewed and it is considered whether there is any impact on the principles for the securities services business from the emergence of DLT.

Finally also in the Appendix, **Regulation** looks at the technology from the regulator's perspective - the benefits of a shared 'golden' transaction record and also the impact of operational requirements for market infrastructures on technology and deployment choices. Various developments led by regulatory agencies around the world are catalogued as well.

After all the work done over the last 12 months, the ISSA working group sees inherent benefits of DLT, some of the more important ones are:

- Reduction of risk
- Reduced, simplified reconciliation
- Operational efficiency
- Single, shared source of trust that could be a valuable foundational data source for machine learning and artificial intelligence applications
- A base to provide potential new revenue generating services

At this point in time there is no live solution yet in the securities services industry, but several are on the horizon which will provide opportunities for the industry to discover which benefits materialize first and which ones are harder to come by.

This report has been written to the best knowledge of the authors and the many experienced work stream contributors. ISSA will monitor the evolution of the adoption and implementation of this new technology and provide regular updates to this initial report.

3 Principles of Governance, Adoption and Integration

3.1 Introduction

There is great interest by individuals, corporations and regulators across the globe in the basic benefits of DLT platforms. At its core, a DLT platform is a distributed, automated, shared database of information and business rules, combined with a methodology for cryptographic protection and ensured integrity of digital data and transactions. But almost all of that interest in the financial industry is focused on models that include clear and formal ownership of responsibility and accountability for that platform.

Establishing DLT as a widespread, accepted platform for the global financial industry and for managing records of public investments will require policies, rules, standards, actions, processes, security, risk and operational controls, best practices, rules of conduct and exception management. All of these requirements are critical to creating and sustaining a financial market network and each of those requirements is ultimately the responsibility of an assigned and accountable governing body for each such network.

It may be argued that establishing "central governance" for a decentralized processing model obviates the need for and value of DLT. But even today's public DLTs have implied governance, which is completely in the hands of arbitrary decisions of a few select programmers and the result has been forks (see also 4.6.1.3), fraud and loss on the network periphery and divergence with the original goals of the 2008 Bitcoin white paper. It is ISSA's contention, aligned with its mission, that DLT plus governance practice aligned with the principles articulated in this paper can substantially improve the "trust but verify" model for the global financial and asset servicing industry.

ISSA expects that DLT will be implemented for many different industries and types of solutions, but financial transactions are unique in that they already have a multi-century legacy of standards, practices, rules, and regulatory oversight, which varies by asset class and jurisdiction. This has been relevant to ensure data quality and consistency through existing models of connectivity and data exchanges across the financial industry and to ensure the safety and soundness of the financial system and the protection of customer assets. This will likely have continuing utility, as the commercial evolution of the financial markets and the emergence of many DLT platforms and vendors indicate that the future will be built on many interconnected ledgers that will need standards and governance to interoperate. There will not be "one ledger with one governance body to rule them all".

There is a range of existing governance models that will continue to have relevance especially for standards (e.g. ISO 20022) that can be leveraged for the emerging DLT models. New governance models will be needed for interoperating with and eventually migrating the existing market infrastructure to DLT, aligned with the new model of distributed data, smart contract encoding of rules and practices, and mathematical models that ensure security, privacy, integrity and auditability. New contract models will be created and new updates, patches and improvements to the core code of the DLT will need to be validated and managed through change and release management practices. Evolutionary enhancements and revolutionary changes in consensus and proof models will inevitably improve all of today's implementations and will require owned and managed deployments. New capabilities will be needed to allow exceptions and problems with immutable smart contracts, which are still the creation of human programmers, to be adjusted and fixed. Forward security as cyber-threats evolve, adjustments for changes in capacity and performance characteristics, network membership, identity management and interoperability and other non-functional requirements all need ownership and accountability.

Most critically, today’s state of DLT, with its inherent characteristics of automatically executing smart contracts and immutability is currently not designed to accommodate exceptions and unanticipated failures of human coding of the smart contracts or of the platform itself, and governance is required to determine how exceptions are managed, disputes are resolved and design flaws are remediated.

Finally, the global financial markets have laws and requirements that vary by country or region, but are each intended to provide protection to the investing public within the jurisdiction of each regulatory body. The continuing evolution of DLT may allow the rules from global policy makers to be encoded within a smart contract platform, but today’s regulatory climate of conflicting and changing laws within and across jurisdictions, and technology built on immutable contracts, limits the applicability of rule automation. So, in the interim, there must be responsibility assigned to ensure that adherence to those rules is monitored and enforced and that ledger networks are managed and monitored for adherence to regulatory guidelines.

DLT, combined with properly implemented and operated governance, has the potential to improve safety and soundness for the financial markets. This section lays out the broad principles recommended for financial institutions to consider and embrace as DLT networks are implemented and adopted for the financial markets.

3.2 Background

3.2.1 Guiding Principles

The guiding principles for the governance of DLTs are to be clear, transparent and promote the safety, efficiency and stability of the system and of the broader global financial system. Roles, responsibilities and accountability should be explicit in a multi-layer DLT environment.

3.2.2 Assumptions

This document has been drafted based on the assumption that the securities industry, as a highly regulated industry, will be operating in a permissioned DLT environment rather than in a permissionless Bitcoin style environment. A key assumption referenced throughout the document is that for each permissioned DLT there will be a central governing body with the responsibility to define membership criteria, membership rules of the infrastructure, of the service or business application under defined roles and responsibilities.

ISSA is working under the assumption that there will not be “one ruling ledger and governance body” rather the expectation that there will be different distributed ledgers implemented by different groups of financial organizations to address different transactions in different asset classes and different regulatory and business requirements. Strong, uniform standards are therefore key for interoperability and the assumption is that the principles should be the same amongst the various operators in the digital environment.

Further assumptions include:

- Smart contracts will need to be governed to ensure that their functionality aligns with business intentions and legal requirements. There is a need for mechanisms that guarantee the integrity of the smart contracts even under stress conditions.
- The issuance of securities will continue according to the same existing rules (e.g. market rules).
- DLT environments must comply with the relevant information security standards, though adapted with DLT specifics in mind.
- Global regulators will continue to explore the benefit(s) that the new technology could bring.

- Rules (regulation / law) will be implemented to insure integrity of the business models including investor protection, entitlements and data privacy.

3.2.3 Distributed Ledgers and the Securities Services Industry

Many private blockchain implementations do not circulate full transactional data to all nodes and have implemented private channels or private space models so only hashes / timestamps are distributed to multiple nodes.
Some private DLT implementations also aim to give regulators access to ledger entries corresponding to entities and transactions those regulators oversee, that the rest of the network cannot see. Although this solution has advantages including immediate transparency and reduced costs for transaction reporting, it would require trust in the regulators' security practices. If a hacker were to gain access to a regulator's node then it could pose a serious threat to the entire network. Thus the regulators having access to the network will have to implement the same security practices as all other participants of the network.

3.3 Considerations for the Governance and Operation of DLTs

Throughout this chapter ISSA explains that providers of services in a DLT environment should be mindful of existing regulations currently in place and should proactively engage with the proper authorities at the earliest opportunity in order to conduct business in accordance with those regulations.

3.3.1 Permissioned versus Open Access Models for DLT for Securities Financial Markets

Business relationships and contracts between players and suppliers in this industry are based on trusted, formal principles of engagement and must be protected and ensured in any DLT environment.

The principal participants that run and operate the infrastructure that provides the securities financial markets systems are tightly regulated and include brokers, exchanges, banks and custodians, administrators, central counterparties, central securities depositories and registrars.

However, end users of the financial markets – investors and issuers - are not generally as heavily regulated with regard to post-trade processing and asset servicing unless they are operating in an intermediary capacity – for example where an investor is an institutional investment fund or an issuer is providing a structured note with underlying issuers.

In the majority of markets, individual investors do not require any regulatory approval to invest in securities or other asset classes; the burden of compliance and oversight generally falls on the intermediaries that provide services. For example, a broker or wealth manager is bound by extensive KYC and client adequacy requirements in terms of clients that it may service. This in turn provides a form of permission-driven eligibility.

Permissionless distributed ledgers are not controlled by any central authority, and in their current form may be vulnerable to a targeted attack (e.g. a 51% attack by a group of miners controlling more than 50% of the network's mining hashrate, or computing power. The attackers would be able to prevent new transactions from gaining confirmation, allowing them to halt payments between some or all users). These characteristics render permissionless systems unacceptable for many critical applications in the securities industry. Private permissioned networks may be deployed in conditions that eliminate these risks entirely.

However, it is important to recognize that these financial markets models may interface with open and non-permissioned systems and networks, for example for cash, where even in today's DLT models there is frequently no formal permission approach to holding cash equivalent asset classes. (A consequence of the above may be, that for the sake of safe DvP transactions only interfaces with permissioned cash networks may be acceptable.)

3.3.2 Roles and Remit (Currently) Performed by Trusted Financial Intermediaries

The following functions and actors, as outlined in business arrangements and contracts, fall into the scope of DLT processes and governance:

- Issuers:
    - Responsible for the issuance of securities instruments and disclosure of relevant financial and operational information into the regulated trading market(s) and via intermediaries to end investors
- Data vendors (securities master information, pricing and other relevant reference data)
    - Primary data vendors
    - Secondary data vendors
- Investors (asset owners)
- Intermediaries acting as distributors
    - Broker dealers
    - Asset managers
    - Fund managers / administrators
    - Prime brokers
    - General clearing members (GCM)
    - custodians
    - Sub-custodians
    - Account operators
    - Network providers (secure network for communications and financial messaging)
- Intermediaries acting as market processors
    - Stock exchanges / trading venues / multilateral trading facilities / OTFs
    - Allocation and matching engines
    - Regulatory reporting repositories
    - Depositary banks
    - (International) central securities depositories ((I) CSDs)
    - Central counterparties (CCPs) (clearing houses)
    - Central banks
    - Cash correspondents
- Regulators (local / regional / global)
- Industry supervisors / authorities:
    - BIS, CPMI-IOSCO, Basel, FSB, …
- Standardization supervisors
    - ISO, SMPG, ISITC, NMPG, …
- Technology providers
- DLT users could define new services (e.g. using smart contracts)

3.3.3 Membership Criteria and Access Control

It is proposed that the central governing body for each permissioned DLT will define the membership criteria and membership rules to which all participants should adhere. With this in mind the following principles should be observed when developing such criteria and rules:

3.3.3.1 Restricting Access to the DLT System to Approved Participants

The existing individual permissioned systems used to run the financial markets have wide-ranging control frameworks to restrict access to information. Approved participants are carefully defined and profiled in terms of formal access to systems and the information contained.

This is made simpler by the make-up of the supply chain model, where only approved members of each intermediary service are authorized for access to each respective system. For example, an exchange will only approve access by its participants; a CSD the same; a bank or custodian by its clients or formally approved 3rd parties.

Under a DLT system it is feasible that the industry will migrate towards an integrated ecosystem model, and hence the model of participant access control will be forced to migrate from a supply chain entity model to one that requires a collective integrated control framework, leading to the following concerns that are discussed in the sections that follow: collective access control model, including access eligibility; proof of identity; and accountability for oversight, monitoring, intervention and escalation.

3.3.3.2 Accountability for Defining Access Eligibility

Market operators should continue to control access to the ledger. Utilizing existing financial markets models with highly defined access eligibility controls, frequently overlaid with tight local regulations that define the criteria for membership. It will be important for new DLT networks to define clear models for access eligibility, noting any compliance requirements under local regulations.

For multi-entity and shared DLT networks, a decision making board will be required to define the access eligibility criteria and any associated identity evidence requirements.

It is highly likely that different participant categories will require different levels of data access and hence a complex model of access eligibility and data access levels may be required.

3.3.3.3 Oversight, Monitoring and Interventions

The DLT network will need to clearly define the process and accountability for access approval processing, ongoing oversight and monitoring of access, including formal audits of activity across the DLT network. This will extend to defining the procedures for interventions and escalation of breaches in conduct.

3.3.3.4 Accountability for Participant Identity Controls and Digital Identity Keys

Proof of identity is an existing industry wide challenge and is a critical area of access control. A DLT network may have a far broader range of participants than existing permissioned systems and without a consistent available approach to identify controls. This includes the need for a hierarchy relationship model, where entities with any form of affiliation are clearly linked.

Furthermore, it is possible or likely that entities will be given authority to operate a client’s digital keys, for example, a custodian may also act as the custodian of an investor or investment fund.

It will be important that the accountability for approving eligible identities is defined and that any external entity identifiers and validated reference data for them (such as the LEI) as well as liability in the event of breaches in execution of this role are clearly listed.

The attributes for identity validation must also be defined to ensure a framework exists for this process. Naturally – where it is available – a digital approach will be preferable.

Mapping against eligibility categories will also be important to distinguish between the access profiles that will be mapped against each participant category.

Key custodianship and protection will also be an important issue, laying out options for maintaining and protecting a client's digital identity keys and how this maps against existing roles such as trustees and custodians. Included in this is the liability for loss of keys and resultant financial impact of such events.

In some instances there will be requests for anonymity and also options to continue to leverage omnibus and nominee structures, both for efficiency and anonymity.

3.3.3.5 In Summary

- Many of the points above are requirements that exist in the current 'non DLT' environment and, as described, will need to continue in a DLT environment (for example the membership criteria for becoming a participant in a DLT system operated by a market infrastructure such as a CSD or a CCP).
- Accountability for all aspects of the DLT Governance should be explicitly specified as part of the services designed.
- Membership criteria is needed for various levels of access including adding new content to the ledger.
- Membership criteria should be set by the governing board or steering committee of each governing entity of a DLT environment. The membership rules could be federated or centralized or a combination of both could apply.
- There is an industry wide challenge around proven identity, and if significant progress is to be made, this can become a key enabler for further opportunities in relation of admission / approval process.
- The DLT environment should have external controls to evaluate the membership criteria to ensure the long term viability of the DLT.

3.3.4 License Rules

The governing body or steering committee ensures that members of the DLT can provide evidence of having the proper license(s) to do business. This should include proper entity legal form(s), regulatory oversight (if applicable) and licenses (e.g. banking license, qualification as custodians).

3.3.5 Network Rules

The network rules should focus on bringing reliability, scalability, availability, security, flexibility, reversibility and operational support dimensions to a DLT business arrangement. These topics can be sidelined as technology topics. The business actors / participants of the securities business value chain on DLT play a key influencing role to ensure the success of these dimensions.

Specifically, in conventional securities business it is highly unlikely to have an unrestricted cryptocurrency type setup. Participation of each actor is already established and is largely driven by existing regulation and standard procedures. In such a context a restricted DLT system with only identified entities that can participate in the network can be envisaged. By using the restricted system, the reliability of the system can be achieved, since malicious intent of business and technical nature by any existing actor is easily identifiable in the network.

DLT comes with the intrinsic feature of multiple copies of the ledger spread across a network of users, so instead of relying on a single authoritative actor, the arrangement is resilient against the failure of a single network node. On the contrary, the value chain in focus may need tiered systems which impose restrictions on the roles that the actors can assume. Such an arrangement will consolidate some crucial functions with a single or restricted set of participants. The availability of these actors should be ensured by the underlying entities that host these actors and by the governing body of the specific DLT arrangement.

Given the distributed nature of the DLT network and participation of actors with different levels of maturity, the security dimension has to be approached cautiously to protect the arrangement from external threats and insider risks. A cryptographic hashing process secures the integrity of the DLT systems and data. However, some data which is not only "need to know" may be shared among the actors on the network. Though such data is encrypted, actors with malicious intent could use brute force to decrypt the data. Use of such brute force is an extremely time and resource consuming undertaking. But outdated encryption techniques can aid such wrong doing.

Since it is more likely to have a restricted network with identified entities for securities business, the network can be attack proofed from direct external risk, but fraudulent transactions could be injected through an existing participant that falls victim to a cyber-attack (e.g. email phishing or malware); it would be no different than today. In such cases liability for such a breach should be covered during the onboarding process by the governing body.

Governing bodies of DLT networks should define the security process controls and the best practices in place and should review them periodically and enforce the changes in the DLT network. It is important that these bodies can bring consensus among the participants in the network regarding security topics. These principles are described in more detail in the information security section.

3.3.6 Node Administration

The governing body or steering committee specifies and documents the various functions that the nodes can perform on the DLT environment.

3.3.7 Change Management / Upgrades

The governing body or steering committee specifies and documents a change management process for changes or upgrades to the network or DLT specifications. The requirement to adhere to this process and to comply with implementation time frames for changes and upgrades to the network or DLT should be incorporated into the contract between the members and the DLT network.

3.3.8 Transactional Finality

An important risk in entering any financial transaction is that the settlement may not take place as expected. Most systems employ a concept of finality, at which point it is believed that the transaction is settled and can't change under any circumstances.

Any system that executes legally significant actions must define finality explicitly in compliance with the existing regulations and laws. If that definition involves risks beyond the basic reliability of the system, these risks must be appropriately managed by the governing body of the system.

3.3.9 Conduct Rules

3.3.9.1 Designation of Governing Entities

The governing body or steering committee needs to put in place and document the process that will be followed to establish and maintain the governing body or steering committee. This will include rules, eligibility requirements for membership to the board or committee, number of members in the board or committee, election and re-election procedures, terms limits, reasons and procedures for removal and dismissal.

The governing body should not make use of information they could gather from the management of the DLT environment

3.3.9.2 Recourse Mechanism

The governing body or steering committee specifies and documents the recourse mechanism for members and participants including how to raise and resolve issues or errors to ensure that the outcome reflects the legitimate intention of transaction participants.

3.3.9.3 Dealing with Fraud and Hacking

The governing body or steering committee specifies and documents procedures for detecting fraud on the services that are provided on the DLT environment as well as the disciplinary actions that should be applied to members or participants committing fraud.

The governing body or steering committee specifies and documents procedures for detecting hacking on the DLT environment as well as the disciplinary actions that should be applied to members or participants committing hacking.

The governing body or steering committee specifies and documents procedures for detecting external intrusion on the DLT environment as well as the necessary measure to protect the existing DLT environment.

The governing body or steering committee establishes the necessary contact with the proper law agencies in the appropriate jurisdictions.

3.3.9.4 Centrally Defined Versus User Defined Automation on the DLT (e.g. Smart Contracts)

If users are permitted to distribute automation codes on the DLT environment, the governing body or steering committee should have a process in place to authorize the functionality of specific smart contracts. Accreditations need to be put in place before the implementation of smart contracts on the DLT environment.

The operating entity of the DLT environment should document when and how they are accountable for with regards to the use of automation codes on the DLT environment.

If automation codes are used in the DLT environment, the governing body or steering committee should ensure that there is a process to address coding errors, or unexpected behavior, as well as mechanisms to allow the code to be halted or terminated in certain agreed scenarios.

3.3.10 Risk

Risks arising from new entrants, partnerships, technologies and competition will emerge and continue to emerge as DLT matures and gains traction. In addition, existing risks currently deemed less material may be magnified by the use of DLT. As such, a review of risk management frameworks and strategies throughout the lifecycle during the adoption and integration of DLT from banks, intermediaries, supervisors, regulators and the FinTech firms themselves will be required.

3.3.10.1 Banks and Intermediaries

These institutions will need to review operational and governance structures, ensure effective IT and adapt risk management processes to address the risks of new technologies and third party governance and oversight of outsourced services.

3.3.10.2 Regulators

Regulators will have to adapt their practices in order to continue their statutory objective of protecting the public interest by contributing to the stability and effectiveness of the eco-system. This may include enforceable regulation in order to identify, manage and monitor risks associated with FinTechs.

3.3.10.3 Banking Supervisors

Guidance should be provided by banking supervisors on how to understand and evaluate risk in a FinTech environment, develop supervisory approaches and identify potential system-wide issues. This may include enforceable standards aiding the identification, management and monitoring of risks associated with FinTechs. In addition, it would be beneficial for banking supervisors to cooperate with other public authorities, like e.g. conduct authorities, data protection authorities, competition authorities and financial intelligence units. Banking supervisors and regulators should learn from each other's approaches and practices and consider whether it would be appropriate to implement something similar.

3.3.10.4 FinTech Governing Body / Steering Committee

These bodies need to absorb the above into their risk and governance framework. This might include mandatory standards that should be attested to by all participants in the DLT.

3.3.10.5 Risk Types for Consideration

The below are the key risks to be considered in a DLT environment:

Transactional Risk
The requirements for the security, entitlements and encryption should all work together to mitigate the transactional risk on the DLT.

Concentration Risk
To avoid excessive risk taking the governing body or steering committee should ensure that, based on credit / activity limits and by considering collateral obligations, concentration risk on the DLT is monitored and controlled.

Credit / Insolvency Risk
To ensure the effective operation and sustainability of the DLT the governing body or steering committee should ensure that there is an agreed protocol for:

- Entry criteria and monitoring of credit worthiness taking in to account credit / activity limits and collateral obligations.
- The treatment and mitigation of an insolvent party which in the concept of a borderless ledger will need firm rules with regards to the legal parameters.

Business Risk
Due to new entrants, partnerships, technologies and competition the risk on incumbent actors' profitability, solvency and stability is significant. Existing actors should ensure:

- Robust strategic and business planning considering the potential impact of FinTechs
- Sound new product and change management approval processes

Operational Risk
These risks will be arising from increased use and dependency on technology. Banks and intermediaries should have effective IT and other risk management processes that address the risks of new technologies and implement the effective control environments needed to properly support key innovations.

Cyber-Risk
Due to the increased interconnectedness the risk of hacking as well as data, operational and technological manipulation will increase. Harmonized supervisory and monitoring standards will be required on a global basis.

Third Party / Vendor Risk
When partnering with third parties and / or outsourcing operational support for technology-based financial services, banks and intermediaries (regulators and supervisors) should ensure that they:

- Have appropriate processes for due diligence, risk management and on-going monitoring of any operation outsourced to a third-party including FinTech firms.
- Maintain controls for outsourced services to the same standard as the services conducted by the bank or intermediary itself.

Regulatory & Compliance Risk
Current bank and industry regulatory, supervisory and licensing frameworks generally predate the technologies and new business models of FinTech firms (see also the regulatory section). This may create the risk of:

- Potential regulatory arbitrage from inconsistent regulatory / supervisory standards and legislation across jurisdictions emanating from the cross-border provision of digital services.
- Lack of clarity in a cross-border context which member state's regime applies.

There is a need for:

- Existing and new regulation to be extended to unregulated firms (FinTechs) and the risk that is presented if this is not the case.
- A review of the interoperability and equivalence of regulations in a borderless ledger.
- Enhanced and universal monitoring and review of compliance with applicable regulations and data privacy law standards (e.g. GDPR).
- Clear allocation of liability across all parties providing parts of a service.
- Cooperation between supervisors is essential to ensure alignment and commonality for cross border activity and e.g. for the treatment of embargoes / sanctions.
- Adequate, consistent disclosure provisions to investors from FinTech firms.
- Adequate, consistent complaint handling procedures at FinTech firms in line with relevant regulations and standards.

Business Continuity Risk / Recovery & Resolution
Due to its decentralized nature, the use of DLT raises questions on how resolution authorities can apply their powers to new technologies and how banks and intermediaries can ensure business continuity if not in control of the system. There is therefore the need to assess the interaction between FinTech and banks / intermediaries and the impact on recovery and resolution planning and policy on a local / regional and global basis including CPMI IOSCO and the Financial Stability Board.

3.3.11 Access by Regulators

Using DLT for recording of transactions in the securities, payments, treasury, FX and possibly other domains could present an opportunity for both the industry and financial regulators. Through the granting of entitlements for viewing transactional and supporting information, rather than having to rely on reporting regimes and data collection, regulators could view with controlled access information on the DLT.

Pulling information by the regulators from DLT by leveraging APIs and financial messaging, could increase the immediacy or transparency and lower the cost of regulatory reporting for the industry.

3.4 Data; Identification, Integration and Integrity

3.4.1 Access Controls

3.4.1.1 Restricting Access to the DLT System to Approved Participants

The existing individual permissioned systems used to run the financial markets have wide-ranging control frameworks to restrict access to information. Approved participants are carefully defined and profiled in terms of formal access to systems and the information contained.

This is made simpler by the make-up of the supply chain model, where only approved members of each intermediary service are authorized for access to each respective system. For example, an exchange will only approve access by its participants; a CSD the same; a bank or custodian by its clients or formally approved 3rd parties.

Under a DLT system, it is feasible that the industry will migrate towards models where there is an integrated ecosystem model, and hence that the model of participant access control will be forced to migrate from a supply chain entity model to one that requires a collective integrated control framework.

This brings to a head a number of core themes that pertain to this collective access control model, including access eligibility, proof of identity and accountability for oversight, monitoring, intervention and escalation. These points are discussed below:

3.4.1.2 Accountability for Defining Access Eligibility

Existing financial markets models have highly defined access eligibility controls, frequently overlaid with tight local regulations that define the criteria for membership. It will be important for new DLT networks to define clear models for access eligibility, noting any compliance requirements under local regulations.

For multi-entity and shared DLT networks, a decision making board will be required to define the access eligibility criteria and any associated identity evidence requirements.

It is highly likely that different participant categories will require different levels of data access and hence a complex model of access eligibility and data access may be required.

3.4.1.3 Oversight, Monitoring and Interventions

The DLT network will need to clearly define the process and accountability for access approval processing, ongoing oversight and monitoring of access, including formal audits of activity across the DLT network. This will extend to defining the procedures for interventions and escalation of breaches in conduct.

3.4.1.4 Accountability for *Participant* Identity Controls and Digital Identity Keys

Proof of identity is a critical area of access control. A DLT network may have a far broader range of participants than existing permissioned systems and without a consistent available approach to identify controls. This includes the need for a hierarchy relationship model – where entities with any form of affiliation are clearly linked.

Furthermore, it is likely that entities will be given authority to operate a client’s digital keys, for example, a custodian may also act as the custodian of an investor or investment fund.

It will be important that the accountability for approving eligible identities is defined and that any external entity identifiers and reference data are clearly listed (such as the LEI).

The attributes for identity validation must also be defined so ensure a framework exists for this process. Naturally – where it is available – a digital approach will be preferable.

Mapping against eligibility categories will also be important to distinguish between the access profiles that will be mapped against each participant category.

Key custodianship and protection will also be an important issue, laying out options for maintaining and protecting a client's digital identity keys and how this maps against existing roles such as trustees and custodians. Included in this is the liability for loss of keys and resultant financial impact of such events.

In some instances there will be requests for anonymity and also options to continue to leverage omnibus and nominee structures, both for efficiency and anonymity.

3.4.2 Trusted Sources of Data

There is a key requirement for data that is introduced to a DLT system to be derived from trusted sources. In the current environment, the majority of industry intermediaries leverage a multitude of data sources and undertake validation and scrubbing exercises to derive a level of confidence on the accuracy of the underlying data. This model is allowed to work, for the simple reason that each intermediary has control over its own data records and in turn can amend or adjust data if it feels that there are inaccuracies. While this may have a client impact; this remains within the control of the intermediary.

In a shared multi-entity DLT network – data introduced to the network will be deemed to be accurate and hence that smart contracts and other transactions lifecycle events can automatically trigger based on the information that is held. There is no concept of amending transactions once executed and hence the impact of inaccurate data drives a need for cancellation and re-booking of such transactions.

Each DLT network must consider who is authorized to introduce data to the DLT network; and what steps and assurances exist for validating the integrity of that data. For example – an entity introducing a new corporate action must undertake a range of validations prior to submitting this into the DLT network.

We will need to consider what liabilities would exist for errors in data submission and paths for resolution of errors in trusted data, and whether the liability for any losses would be passed to the users of the network or retained with the trusted data provider. Recognizing that this may make the system potentially unattractive to any data vendors.

There could be an option for a DLT network to put in place a way for multiple entities to create a smart contract around introduced data; where multiple parties must match new data for it to be validated; but this seems to be a weak model for data introduction.

3.4.3 Application Programming Interfaces (APIs)

The governing body or steering committee should publish a list of purposes for APIs to be used with the DLT. In accordance with the standards section below, APIs based on standards only should be used and principles and guidelines to develop APIs on the DLT should be published. The governing body or steering committee should document a process to review and to test APIs before they are implemented within the DLT.

3.4.4 Data on the DLT

3.4.4.1 Validation of Identity and Integrity of Messages on the DLT

The governing body or steering committee should ensure that a process is in place to validate the identity of members and participants using the DLT. The governing body or steering committee should have a process in place to address situations when someone tries to access the DLT and is not recognized as a validated member.

The governing body or steering committee should ascertain that processes are in place to ensure the security of identification and authentication and integrity of any data on the DLT.

3.4.4.2 Data Privacy and Sensitivity

The governing body or steering committee should ensure that there are entitlements in place to ensure the privacy and the rights to view the details of transactions on the DLT.

3.4.4.3 Regulatory Issues on Data Privacy

There is a growing level of regulation on data privacy in local country laws. The DLT network solutions that cover multi-national participants will require a clear approach to ensuring compliance with the respective laws. This may need to consider the location of DLT nodes and the extent that these equate to holding of data in each country / jurisdiction.

It is worth noting that even an encrypted version of personal data may still be considered personal data – and be subject to the rules on data privacy.

The industry finds itself in an interesting set of divergent priorities in terms of regulatory oversight. From one angle there is a need to protect and restrict data in the DLT network from unauthorized access, while at the same time there is a demand from relevant regulatory bodies for oversight and transparent reporting.

Models need to balance the need for data protection with the need to allow regulators the right level of access to complete their duties.

3.4.4.4 Sensitivity of Data

Not all data held in the DLT network will have equal sensitivity, and hence the impact of breaches in data protection and privacy will have different risks and outcomes.

It is important for DLT network designers to assess the sensitivities of data, also recognizing that packages of data will have different profiles of sensitivity than each underlying data component. For example; the packing of identity, stock name and trade details have a far higher sensitivity than each data component in isolation.

3.4.4.5 Restricting Data Held on the DLT Network

The final approach to data protection is simply to restrict the amount of data held within the DLT network, so that even in the event of unauthorized access to the network, limited private data can be accessed. This approach is gaining traction where a third party and trusted repository for information holds a sub-set of data and only selected parties are provided with the authority to access this data.

Naturally, this also presents an issue to ensure that trusted repositories are clearly defined and that data within these in turn comply with the highest levels of data encryption and protection.

3.4.4.6 Legal Basis of Records

There may be a requirement for a DLT network to determine which data record within the multi-node model is the legal data record. This may need to comply with the local regulatory themes on data being held locally and other aspects. But in the event of a dispute it may be important that a single data point is considered to be the legal record. This introduces a theme where all data records may not be the same and where selective records carry a higher standing. This may become important when assessing finality of a transaction e.g. under UK law.

3.5 Business Standards and Integration

3.5.1 Principles for Maximizing Interoperability

In a networked business such as finance, interoperability between different players and platforms is critical. Business processes or value chains are composed and recomposed from multiple actors, infrastructures and systems. For this to happen safely and efficiently, standardization is required at multiple levels, from standard communication protocols to standardized business data.

As DLT evolves and is deployed in the securities industry, it will take its place in these extended value chains, replacing or supplementing existing steps and processes. It is therefore important that DLT and its implementations are designed to integrate with each other and with existing automation mechanisms. To achieve this, it will be necessary to adapt existing standards to the requirements of DLT and to develop new standards that address the capabilities that are unique to this technology.

A standards 'stack' could be considered, where the lower levels provide technical interoperability, supporting higher levels that are concerned with business data semantics and common processes.

Technical interoperability is a cross-industry concern, and technology vendors, open source initiatives and standards bodies are devoting much effort to developing standards in this area, including 'interledger' protocols, which allow simple business transactions to be coordinated between ledgers[1]. The International Organization for Standardization (ISO) has created a new technical committee (TC 307) with a mission to create cross-industry DLT standards, starting with foundational work on common terminology and reference architecture.

The securities industry already makes extensive use of business standards to streamline its processes, including FIX in the pre-trade space, ISO 15022 and its successor ISO 20022, covering post-trade through asset servicing. Use of these standards has conferred great benefits on the industry in terms of efficiency, cost and risk reduction. But these benefits were not easily won. Many securities markets started their automation journey with proprietary 'home grown' formats, and it has taken costly migrations and substantial re-engineering to converge to common standards.

The challenge for the industry today, as it embraces DLT, is to avoid the mistakes of the past and to consider standardization and interoperability from the outset. Happily the existing standards provide more than an example; there is much of value in today's standards that can be re-used in a DLT context.

Recommendations:

1. DLT technology vendors targeting the securities industry should collaborate under the auspices of standards bodies and open source initiatives to ensure that DLT platforms are interoperable at a technical level;
2. The technical standards community, such as ISO/TC 307, should facilitate this work by providing foundational standards, aimed at simplifying communication and collaboration between technical teams;
3. DLT technology vendors should consider the importance in their offerings of providing easy integration with existing automation technology such as messaging gateways, standard middleware and APIs.
4. The securities industry should collaborate to evolve and adapt the business standards that will be required for DLT to take its place in securities value chains and business processes with minimum disruption and rework.

3.5.2 Applicability of Existing Financial Standards to DLT

Today's business standards fall into two broad categories:

- **Reference data standards** define universal codes for key data elements such as currencies, legal entities or securities. They define both the format of the data (e.g.

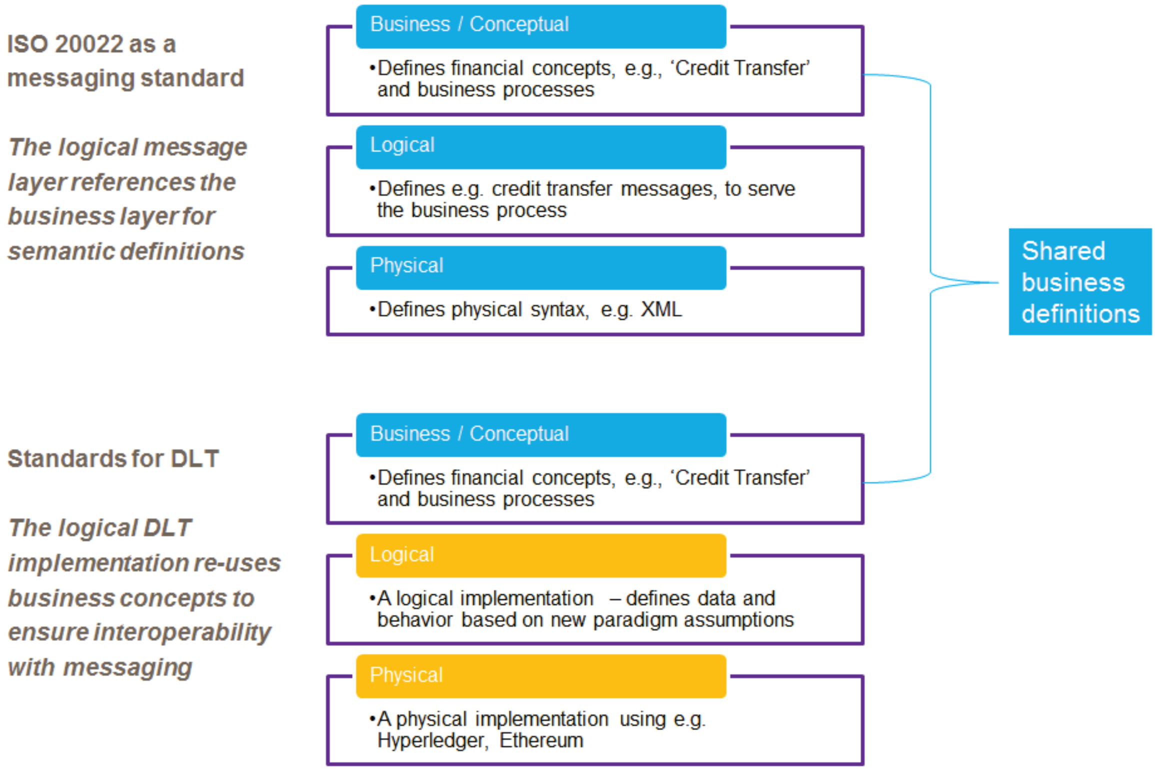
[1] https://www.w3.org/community/interledger/

the length and format of a currency code; the attributes required to describe a currency) and the data itself (e.g. the list of agreed currency codes, 'EUR', 'USD', etc.). Reference data standards ensure consistency for important business data.

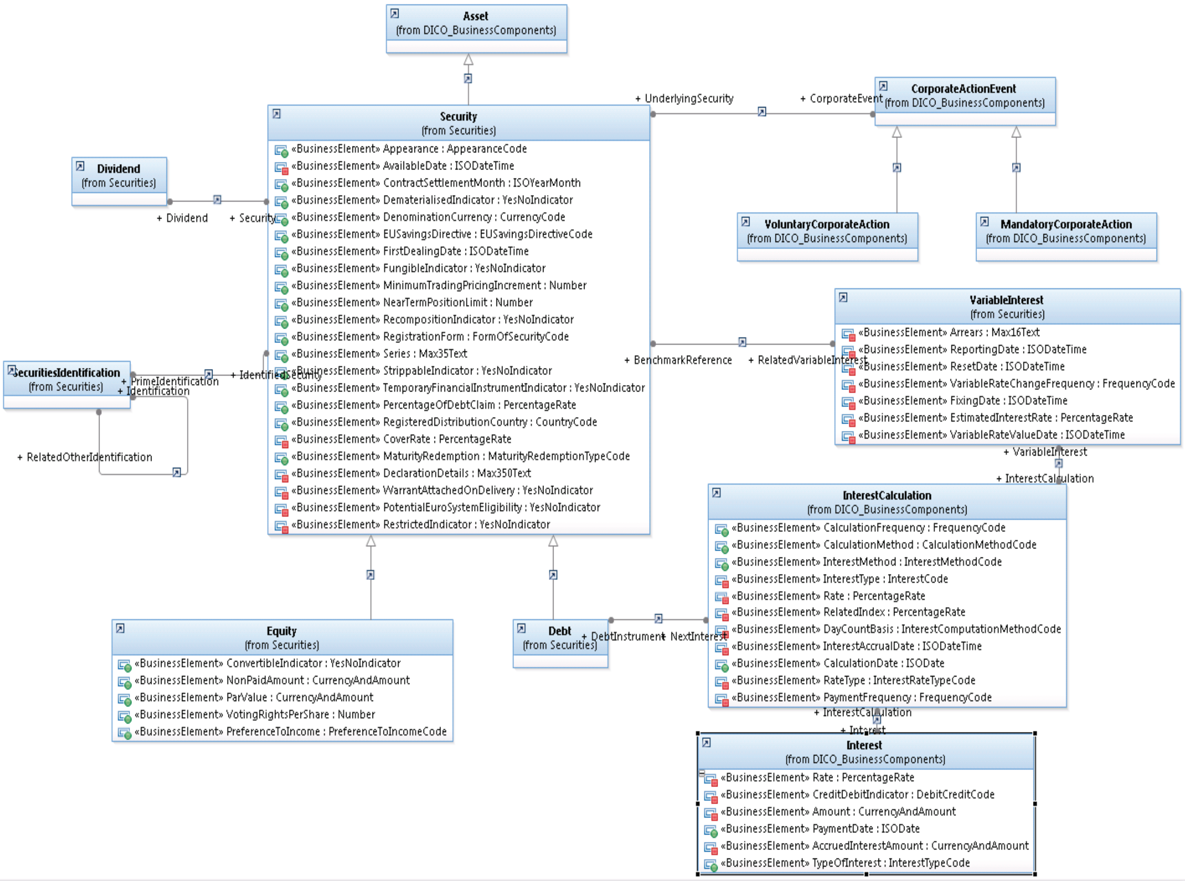
- **Messaging standards** describe formally the content of business messages exchanged by industry participants to complete business processes, such as payment initiation and securities settlement. They also describe the roles played by different actors in a business process and the message flows required to achieve a particular automation goal. Messaging standards specify data elements using reference data standards wherever possible to minimize ambiguity.

Both reference data and messaging standards can be re-used in a DLT context. For reference data this is reasonably straightforward, for example wherever a currency needs to be identified on the ledger, a standard country code should be used. For messaging, re-use is more complicated, because the automation paradigm of DLT – where data is shared automatically amongst authorized parties - is very different from point-to-point message passing. The commonality is not in the message structures but in the semantics of the business data shared.

One widely used messaging standard – ISO 20022 – separates business semantics formally from the message definitions exchanged by users. ISO 20022 defines a layered architecture, where the top layer is an abstract model of key business concepts that is independent of any automation mechanism. This then seems a good place to look for content that can be shared and re-used in a DLT context. The diagram below illustrates the separation of business definitions from messaging concerns in the ISO 20022 standard and how these definitions might be re-used in a DLT context:


ISO 20022 as a messaging standard
The logical message layer references the business layer for semantic definitions
Business / Conceptual
•Defines financial concepts, e.g., 'Credit Transfer' and business processes
Logical
•Defines e.g. credit transfer messages, to serve the business process
Physical
•Defines physical syntax, e.g. XML
Shared business definitions
Standards for DLT
The logical DLT implementation re-uses business concepts to ensure interoperability with messaging
Business / Conceptual
•Defines financial concepts, e.g., 'Credit Transfer' and business processes
Logical
•A logical implementation – defines data and behavior based on new paradigm assumptions
Physical
•A physical implementation using e.g. Hyperledger, Ethereum

For example, the diagram below (using the Unified Modeling Language, UML) is an extract from the ISO 20022 business model for securities. It indicates via specialization that a security is a kind of an asset and that a debt instrument (or bond) is a kind of security. Further, it shows the attributes common to all securities and the attributes specific to debt instruments, including the details of the calculation information that needs to be specified for interest (coupon) payments. Some attributes (or business elements) are defined as simple types, like text strings, others are typed by other structures (business components). For example, a party – say, the "bond issuer" - is defined by a business component that specifies name, address and other identifiers such as business identifier code (ISO 9362 BIC). Each business element and business component is fully described, in English, in the business model.


Asset
(from DICO_BusinessComponents)
+ UnderlyingSecurity
+ CorporateEvent
CorporateActionEvent
(from DICO_BusinessComponents)
Security
(from Securities)
«BusinessElement» Appearance : AppearanceCode
«BusinessElement» AvailableDate : ISODateTime
«BusinessElement» ContractSettlementMonth : ISOYearMonth
«BusinessElement» DematerialisedIndicator : YesNoIndicator
«BusinessElement» DenominationCurrency : CurrencyCode
«BusinessElement» EUSavingsDirective : EUSavingsDirectiveCode
«BusinessElement» FirstDealingDate : ISODateTime
«BusinessElement» FungibleIndicator : YesNoIndicator
«BusinessElement» MinimumTradingPricingIncrement : Number
«BusinessElement» NearTermPositionLimit : Number
«BusinessElement» RecompositionIndicator : YesNoIndicator
«BusinessElement» RegistrationForm : FormOfSecurityCode
«BusinessElement» Series : Max35Text
«BusinessElement» StrippableIndicator : YesNoIndicator
«BusinessElement» TemporaryFinancialInstrumentIndicator : YesNoIndicator
«BusinessElement» PercentageOfDebtClaim : PercentageRate
«BusinessElement» RegisteredDistributionCountry : CountryCode
«BusinessElement» CoverRate : PercentageRate
«BusinessElement» MaturityRedemption : MaturityRedemptionTypeCode
«BusinessElement» DeclarationDetails : Max350Text
«BusinessElement» WarrantAttachedOnDelivery : YesNoIndicator
«BusinessElement» PotentialEuroSystemEligibility : YesNoIndicator
«BusinessElement» RestrictedIndicator : YesNoIndicator
Dividend
(from Securities)
+ Dividend
+ Security
VoluntaryCorporateAction
(from DICO_BusinessComponents)
MandatoryCorporateAction
(from DICO_BusinessComponents)
VariableInterest
(from Securities)
«BusinessElement» Arrears : Max16Text
«BusinessElement» ReportingDate : ISODateTime
«BusinessElement» ResetDate : ISODateTime
«BusinessElement» VariableRateChangeFrequency : FrequencyCode
«BusinessElement» FixingDate : ISODateTime
«BusinessElement» EstimatedInterestRate : PercentageRate
«BusinessElement» VariableRateValueDate : ISODateTime
+ BenchmarkReference
+ RelatedVariableInterest
SecuritiesIdentification
(from Securities)
+ PrimeIdentification
+ Identification
+ IdentifiedSecurity
+ RelatedOtherIdentification
+ VariableInterest
+ InterestCalculation
InterestCalculation
(from DICO_BusinessComponents)
«BusinessElement» CalculationFrequency : FrequencyCode
«BusinessElement» CalculationMethod : CalculationMethodCode
«BusinessElement» InterestMethod : InterestMethodCode
«BusinessElement» InterestType : InterestCode
«BusinessElement» Rate : PercentageRate
«BusinessElement» RelatedIndex : PercentageRate
«BusinessElement» DayCountBasis : InterestComputationMethodCode
«BusinessElement» InterestAccrualDate : ISODateTime
«BusinessElement» CalculationDate : ISODate
«BusinessElement» RateType : InterestRateTypeCode
«BusinessElement» PaymentFrequency : FrequencyCode
Equity
(from Securities)
«BusinessElement» ConvertibleIndicator : YesNoIndicator
«BusinessElement» NonPaidAmount : CurrencyAndAmount
«BusinessElement» ParValue : CurrencyAndAmount
«BusinessElement» VotingRightsPerShare : Number
«BusinessElement» PreferenceToIncome : PreferenceToIncomeCode
Debt
(from Securities)
+ DebtInstrument
+ NextInterest
+ InterestCalculation
+ Interest
Interest
(from DICO_BusinessComponents)
«BusinessElement» Rate : PercentageRate
«BusinessElement» CreditDebitIndicator : DebitCreditCode
«BusinessElement» Amount : CurrencyAndAmount
«BusinessElement» PaymentDate : ISODate
«BusinessElement» AccruedInterestAmount : CurrencyAndAmount
«BusinessElement» TypeOfInterest : InterestTypeCode

This content, suitably filtered, modified and supplemented, can be used by implementers of business solutions based on DLT to define the information on the ledger itself, or at least the data exchanged via APIs or other mechanisms used to expose the DLT solution to its users, human and automated. The benefits are twofold:

- Avoids 're-inventing the wheel' in terms of business definitions;
- Facilitates interoperability amongst DLT implementations and with existing financial industry infrastructure including electronic messaging.

Recommendations:

1. Designers of DLT solutions for the securities industry should understand the existing landscape of business standards, re-use reference data standards where they exist and look to the business semantics captured in messaging standards to inform their solution designs and APIs;
2. ISO 20022 is a widely deployed modern standard with widespread coverage of securities and other financial business domains and an architecture that separates business semantics from messaging. As such, ISO 20022 is a good starting point for designers of DLT solutions looking for standard business definitions or concerned with end-to-end interoperability.

3.5.3 Candidates for New Standards as the Technology Matures

As noted in the section above, while existing standards may be useful in the context of DLT, the new technology proposes a different automation paradigm for which no business standards currently exist. For example, there is no standard, neutral way to define or represent the behaviour of a smart contract, or the parties that participate in a contract and their rights and obligations. As the technology matures and best-practices emerge, we can expect these to be formalized in some commercially neutral standards.

Recommendations:

DLT vendors, securities industry implementers and users need to collaborate through neutral standards organizations such as ISO to develop DLT-specific business standards that maintain compatibility at the data semantic level with existing industry standards, including:

a. Standards definitions for securities industry business concepts and processes;

b. Common definitions (templates) for smart contracts;

c. Common mechanism for cross-referencing legal and smart contracts

3.6 Main Conclusions

The use of DLT places a heightened importance on the governance models by establishing clear lines of responsibility. Accountability of all aspects of the DLT governance should be explicitly specified as part of the services designed. Transaction finality is a key constituent of existing models, and DLT systems must be able to define finality in compliance with existing regulations and laws. A framework for DLT risk assessment should be considered as should data privacy and GDPR themes. Interoperability between market participants, platforms and related outside infrastructures should be considered from a control and governance perspective.

4 Information Security

4.1 Guiding Principles

The guiding principles for information security of DLTs should provide a clear set of guidelines to promote the protection and security of information held with DLT systems or how these interact with non-DLT systems.

4.2 Scope of Information Security Stream

The information security stream has been refocused to look primarily at the more technical aspects of information and data security that distributed ledger systems pose. There are a range of themes that overlap with the governance stream and a decision was taken to cover these primarily in the governance stream section.

On this basis the focus is on the following core themes.

- Data confidentiality
- Data integrity
- Smart contract security
- Digital identity keys
- Disaster recovery and back-ups

4.3 Introduction to Information Security

The implications for information security in the new paradigm of distributed ledgers are paramount to financial institutions adopting this rapidly evolving technology. For the purpose of this paper, the focus is on "permissioned ledgers", those that only contain known entities participating in transaction validation and not the "permissionless ledgers", such as Bitcoin or the public Ethereum network.

The bulk of the focus continues to be on how to handle data confidentiality in a system designed to be a shared source of truth. There are various different approaches to achieving confidentiality but each have implications for data integrity, ensuring that data is consistent across the network in near real-time. Just as institutions need to maintain the same confidentiality levels required of them today, they must avoid maintaining the same 'siloed' data stores that lead to many of the issues that DLT is seeking to solve. The report examines the tradeoffs in the spectrum between total confidentiality and total integrity.

Another key area of focus for security professionals is on the safety of smart contracts and their associated languages. This is an important area that has received relatively little attention despite well publicized exploits costing tens of millions of dollars on the corresponding public blockchain networks. ISSA expects to see an increased focus on smart contract security in the coming years as each of the most predominant DLT platforms support different languages and approaches.

This section concludes with covering the implications for the maintenance of digital identity keys and the implications of DLT for disaster recovery and backups. It considers the inherent properties of a DLT system for performing disaster recovery and replications and how digital identities affect both the data confidentiality and integrity properties of the system.

ISSA aims to provide an overview of the key information security building blocks and the different approaches being taken by different solutions at the time of writing. These are likely to evolve rapidly over the next few years as refinements and improvements are made to improve security, confidentiality, integrity and smart contract languages.

4.4 DLT Model Context

It is useful to reflect on the core differences and challenges that DLT models have over existing "segregated" ledger models and approaches when assessing information security. There are a number of challenges that changing the security servicing model to DLT poses, and the following sections look at the approaches that are being developed to address these differences.

In existing non-DLT models the industry operates under a broad segregated ledger model, where each entity maintains its own distinct version of the 'truth' and where this view of the truth is adjusted and validated by a range of transaction authentication and reconciliation processes.

Data confidentiality and security is achieved by each industry participant maintaining its own distinct platforms and firewall protections and individual databases, where access both internally and externally is highly permissioned. Data is only shared with direct contractual counterparts within the permissioned network, with data generally restricted to a firm's relevant activity and where each networked participant is responsible for its own approach to internal and external data security and data access. Collective ecosystem data security is therefore a reflection of multiple bilateral arrangements rather than a single integrated model.

Data integrity is achieved through secure transaction media and extensive bilateral processes of reconciliation of each firm's ledger view. Firms leverage secure communication media, such as SWIFT, to allow for messaging to facilitate automated transaction processing, leveraging a secure set of digital identity keys, high grade message encryption and internal protocols to determine a transaction's authenticity. Reconciliations of positions and transaction records are undertaken bilaterally between counterparties and with service providers/ clients, and any consensus of positions is indirectly the result of multiple bilateral affirmations rather than a broader agreement.

There are added challenges in affirming data integrity under existing models, where the use of both omnibus and nominee account structures by some account holders and segregated accounts by other account holders and the lack of full end investor transparency across the ecosystem can hinder the ability for a broader record reconciliation.

Firms may use bespoke macros and algorithms to determine and automate processing or decision outcomes, and these are generally created by and for each participant with adjustments in position reflected primarily on that participant's ledger. It is rare for these to be audited or reviewed by external parties, and these generally remain internal.

The base model of DLT (e.g. Bitcoin) generally envisages a single permissionless network for DLT, where the emphasis in system design was placed on data integrity rather than data confidentiality, and where consensus models dominated the design focus.

The financial services industry already operates under a highly permissioned model, and hence the evolution of DLT models for this sector has sought to adjust and tailor the design features to achieve at least the current levels of information security protection, including both data confidentiality and data integrity.

DLT presents a number of core challenges related to information security that viable models need to address.

Data Security and Confidentiality
The need to restrict data access to relevant counterparties and regulatory authorities and avoid broader sharing of confidential data with other parties in the network.

Developing common models for data encryption and cryptography across a network, rather than this being bilateral models between counterparties.

Data Integrity
Developing efficient models for real-time and high capacity processing, while retaining a necessary level of transaction and data validation.

Developing models for authenticating transactions in permissioned and trusted participant models, while avoiding the latency and cost of heavy consensus approaches used in permissionless models.

Developing procedures and models that cater for situations where records do not align or reconcile across the ledger or to simply correct mistaken transactions.

Smart Contracts
The requirement for a common and transparent approach to rules covering the manner that adjustments are made to the shared state or common ledger.

Disaster Recovery
Clear models are needed for disaster recovery across the network, and models for determining the base records for any recovery.

The following sections look at the options and approaches to address these challenges and models that are being used by leading providers and platforms in the information security space.

4.5 Data Confidentiality

Maintaining the same level of data confidentiality in DLT as exists today in traditional systems is a prerequisite for their adoption within financial services. At first, the notion of confidentiality on a shared ledger seems contradictory to the original intent of the blockchain technology underlying Bitcoin, but this area has been the primary area of research for vendors focusing on the enterprise space, particularly in financial services. It is important to note that how confidentiality is achieved has consequences for other properties of the system, such as network-wide data integrity and the ability to combine disparate smart contracts to create continuous processes.

At a high level, methods to ensure confidentiality fall into two categories: "on-chain data", attempts to conceal all or part of sensitive data that is replicated to multiple participants and "off-chain data", the sharing of sensitive data directly with only those entities entitled to view it but using a blockchain, or cryptographic data structures generally, to coordinate and confirm validity of this data. The following options are not mutually exclusive and a combination is used in some solutions.

4.5.1 On-Chain Data

4.5.1.1 Disjoint Networks

One solution to on-chain data being replicated to all participants in the network is to create multiple distinct networks or subnets each with their own blockchain so that only the participants in that network are able to view the on-chain data. Hyperledger Fabric 1.0 introduced the notion of "channels" deployed as fully disjoint networks with separate endorser sets and ordering nodes for the purpose of conducting private transactions between two or more specific members. Transaction data and smart contracts are executed within these separate channels.

Disjoint networks, essentially distinct blockchains, solve the issue of confidentiality provided that all related transactions and smart contracts can be visible to all participants on that network. However, this is not always the case as entities need selective visibility, often referred to as partial disclosure, into a particular transaction or step in a smart contract process but not its entire history. R3 used the analogy of slack channels, where once a participant is added, all previous history and future conversations become visible to that participant, an all or nothing proposition. Further, it also introduces a coordination complexity between disjoint networks as an asset may need to be moved between networks with different participants, the integrity of which is difficult to prove without a common provenance.

4.5.1.2 Encryption

A potential solution to reconcile DLT with access restriction is to encrypt all sensitive data on the ledger, controlling the keys by which it may be decrypted. The technology that applies hierarchies of keys is sufficiently well-researched and can be used to both guarantee good cryptographic properties and enough convenience to manage access rights efficiently.

Universal availability of data still brings challenges, however, even with encryption. Vast amounts of available data make it possible to run correlation analyses between encrypted pieces of data, detecting patterns that may betray sensitive information. Techniques exist to protect against this kind of analysis, but it is important to understand that even the use of the simplest operations like password salting can significantly increase network overhead.

There are many different techniques for encrypting data. The majority do not allow to perform operations on the encrypted data until it is decrypted, which limits the value of replicating the data as no transaction validation can be performed on it without the data being decrypted first. Hyperledger Fabric 1.1 enables the option to encrypt sensitive data within channels, so that only the peers privy to that data can decrypt it and verify its contents before it is submitted to an ordering service. Other techniques, such as homomorphic encryption, allow computation on part of the encrypted data which gives a result that matches as if it had been performed on plaintext. This allows for a level of transaction validation, such as ensuring the number of inputs matches the number of outputs so that no new assets can be created. An example of this is "confidential transactions", developed by Blockstream for the Bitcoin protocol and modified by Chain named "confidential assets" for their permissioned networks.

However, replicating encrypted data to entities not entitled to view it presents several security challenges, aside from the regulatory issues with data domicile rules and duty to protect client information. The first is, that big data techniques and network graph analyses can be performed to discover patterns and relationships across a large scale data set to infer or reveal information, such as trading patterns or payment volumes. The second is forward secrecy: if an analysis reveals sensitive information, keys are compromised or advancements in computing break the encryption scheme, this could allow competitors to decrypt your information on their servers without your knowledge on a real-time basis. Even if any compromises were identified and fixed, the fix would only apply to future data and not historical data up and until that point in time.

Lastly, there is a third concern that currently significantly undermines the security of DLT systems that rely on encryption techniques to preserve confidentiality. In traditional software development all critical security systems and processes are typically taken from off-the-shelf solutions and not developed as a part of business application. It is done for a good reason – there are many pitfalls in implementing security protocols, and missing even one can create dangerous vulnerabilities. For DLT, which is a technology in an early phase of development, enterprise-grade solutions don't yet or are just starting to appear. Most implementations are done in-house by innovation teams, which all but guarantees that these systems will have exploitable vulnerabilities.

4.5.1.3 Zero Knowledge Proofs

Zero knowledge proofs (ZKP) are a relatively new cryptographic method in which one entity can prove to another that a particular property is true without sharing any information about how they know that property is true. A variant of this is zk-SNARKs and zk-STARKs, which enables ZKPs without the need for the prover and verifier to interact. The most well-known example of zk-SNARKs in this field is the anonymous cryptocurrency, Zcash. The technology behind Zcash, the Zero-knowledge security layer (ZSL), was incorporated into J.P.Morgan's permissioned Ethereum derivative, Quorum, as an option for use in private settlements validated by the network.

Zero knowledge proofs have a lot of potential for use within DLT. However, as they currently stand they are very computationally intensive to generate and are not performant at scales needed in financial services. Academic research and practical usage is relatively limited compared to other cryptographic techniques and as it is such a complex field, there is a lot of potential for errors to occur. Lastly, when an implementation error is inevitably found, there is no method to perform forensic analysis to verify an exploit. This risks undermining the trust in an operating network as, by design, there is no way to discover if an exploit has occurred.

4.5.2 Off-Chain Data

Other approaches to Data Protection are to simply restrict what data is replicated on the blockchain or across the network, so that even in the event of unauthorized access, limited data is exposed. This approach is gaining traction where entities hold a subset of data that pertains to them but they can be sure that the cross section of their subset and their counterparties' subsets are identical.

4.5.2.1 Uniqueness Services

The role of Uniqueness Services is to order transactions and prevent double spends in a network without replicated on-chain data to validate. Uniqueness services may also validate the contents of a transaction and could be operated by a single entity or decentralized across multiple organizations. In Hyperledger Fabric these are called "Ordering Services" and in R3 Corda, "Notaries". As the name implies, the primary role is attesting the uniqueness of a transaction, that inputs to the transaction have not already been consumed, and the quantity of assets in the inputs match the outputs and that they are valid. Uniqueness services provide the point of finality in a given network; until a transaction has been notarized (cryptographically signed) by the service, the network cannot rely on its validity.

While uniqueness services can be decentralized by the addition of pluggable consensus, this reintroduces some of the challenges of on-chain data examples given above, as information must be shared with multiple entities. Most implementations therefore rely on a single uniqueness service, and as such this represents a single point of failure.

4.5.2.2 One-Way Cryptographic Hashes

Unlike encryption, in which data can be decrypted, cryptographic hash functions are one-way and infeasible to revert. They are a mathematical algorithm that takes any arbitrarily sized input and outputs a fixed-length string, called a hash (sometimes referred to as a "commitment", "digest", or "fingerprint"). There are many different hash function implementations, with the "ideal" functions having certain properties:

- Always outputting the same hash for a given input (deterministic);
- Being inexpensive to generate and infeasible to brute force;
- Ensuring a minor change to the input outputs an uncorrelated hash;
- It being infeasible to find two different inputs which generate the same hash (a hash collision).

By sharing an ordered, replicated set of hashes on a blockchain across the network, but only sharing the corresponding sensitive data privately to the entities involved, data confidentiality can be preserved without losing the network-wide integrity of a shared, replicated ledger. These simple hashes can also be extended to merkle trees to combine the fingerprint for off-chain data with shared secret notification sets so that all entities can not only know that what they see is what their counterparties see, but be sure that they are not missing any data relevant to them. This design has been implemented by the Digital Asset Platform with their implementation of the global synchronization log. Quorum later adopted a similar option alongside network-wide public transactions and zero knowledge proofs. Hyperledger Fabric is also working towards adding this approach.

4.6 Data Integrity

Systems in use in financial services today optimize for data confidentiality. The most obvious example at the other end of the privacy spectrum is the public Bitcoin blockchain. The design of Bitcoin deliberately made trade-offs to confidentiality in order to achieve maximal integrity, by making all transactions visible and verifiable by anyone. As noted, the data confidentiality model used has major implications for the integrity state of the network or sub-networks within a DLT system. As such, there are various differing approaches to ensuring integrity which also fall into two high level categories: "pre-commit validation", verifying transactions are valid before they are committed to the ledger and "post-commit validation", giving authority to certain entities to commit transactions to the ledger but allowing all participants to independently and provably verify the validity of transactions pertaining to them. Both classes of integrity models make trade-offs, which are discussed below.

4.6.1 Pre-Commit Validation

4.6.1.1 Multi-Signature Authorization

The simplest approach to ensuring the validity of transactions is to require all entities, including the uniqueness service where appropriate, to cryptographically sign all transactions before they are committed to the ledger - commonly referred to as "multi-sig". This provides a provable record that all entities agreed to the transaction or update that can be independently verified by others through the use of public and private key cryptography.

While elegant in its simplicity, a significant drawback of this approach is that signatures must be applied at runtime, the point in which a transaction occurs. This introduces a new form of systems interdependency between entities as the downtime of one entity, or even deliberate withholding of authorization, could prevent the progression of a certain process, even if that entity's authorization is not required. In financial services, this can have severe knock-on effects including race conditions, front running and blocking batch processes such as netting.

4.6.1.2 Consensus Algorithms

Consensus algorithms shift this burden from the entities involved in the transaction to the entities responsible for validating transactions, and only require a majority of validating entities to approve a transaction before it can be considered committed. It is important to note that the commonly used term "consensus" in the DLT industry typically is used as shorthand for "Byzantine Fault Tolerant Consensus (BFT)", which can handle a certain level of malicious behavior, rather than the traditional fault tolerant consensus, which can only handle technical issues such as crashes or network interruptions. The majority of enterprise DLT systems leverage fault tolerant consensus for high availability, regardless of whether they support BFT consensus. For the purpose of this paper, "consensus" is used to mean BFT consensus.

The primary purpose of consensus algorithms is to provide censorship resistance or alleviate the need for a trusted entity. Consensus algorithms allow any entity participating in its consensus group to append a block to the blockchain for validation by the rest of the network. Only once minimum thresholds of consensus nodes, depending on the protocol used, have accepted the block, are the transactions it contains considered committed. Some consensus algorithms permit transaction finality and others make it increasingly unlikely that a transaction will be reversed with each additional block appended. Consensus algorithms allow for a certain number of nodes to be faulty or even malicious and for the network to still proceed with integrity. The number of nodes that are required to collude to halt the progress of the ledger depends on the protocol used.

However, consensus algorithms each have their own trade-offs, and their applicability for certain use cases are a topic of debate. To give an illustrative example, if the European Central Bank initiates a transaction on its RTGS system and is the sole authority of which entities own what quantities of central bank euros, it is questionable whether employing a consensus algorithm across multiple central banks provides benefits. In cases where there already exists an authoritative entity that has legal responsibility for the maintenance of a ledger, there should be careful consideration as to the business case of utilizing a consensus algorithm. The choice of the consensus algorithm, if any, should always be made with the profile of the users of the ledger, their incentives, legal liabilities and requirements of the business application run by the ledger.

Appendix 3 "Information Security" provides an overview of the different forms of consensus algorithms, and options and considerations for industry professionals when deciding which approach to take.

4.6.1.3 Consensus Failures

It is important when assessing different approaches to consensus models that participants understand the range of issues that can be caused when a consensus model fails and how each blockchain platform addresses these issues.

Forks: a blockchain fork results in different nodes converging on a different set of blocks and hence consensus is compromised and the ledger is split from a certain point in time. This can occur from basic system latencies, where 'orphan blocks' occur when two different but valid blocks are broadcasted at the same time. They are usually dealt with as soon as a new block is added to one of the chains and the network accepts the longest chain as valid and discards the orphan block. But it is important that the system has the mechanism to converge on a single chain, or this will compromise the integrity of the chain if inconsistent data is recorded.

Consensus failures: consensus failures are situations where nodes fail to reach a consensus where the algorithm requires a pre-agreed majority. This can be triggered by node network failures, non-compliant nodes or more systemically where nodes cannot make decisions due to the nature of messages sent from other parts of the network.

Dominance: where consensus outcomes are open to manipulation by a single or group of entities. A system should be able to be resilient against Sybil attacks, where control is artificially created by a select number of nodes creating dominance in the consensus algorithm by generating a breadth of identities that they ultimately control.

Cheating: where validating nodes independently maintain parallel forks in the blockchain of fraudulent transactions. This parallel fork is then presented as proof to the "auditor" of fake transactions going through. The blockchain algorithm must be designed with the capability to make sure such parallel fork attacks are unable to develop.

Poor / slow performance: where excessive time is required under certain conditions for consensus to be achieved either due to malicious intent or network latency.

4.6.2 Post-Commit Validation

An alternative to the use of pre-commit consensus algorithms in permissioned enterprise usage is to assign privileges to existing entities that have the sole legal responsibility to maintain their ledger but to allow all parties to that ledger to independently verify all transactions that pertain to them. Rather than the "don't trust anyone" approach of byzantine fault tolerance, post-commit validation is more akin to a "trust but verify" model. In this model, the operators of the ledger act as "provers" and all participants act as "verifiers". An example that supports post-commit validation in addition to pre-commit is the Digital Asset Platform. As all transactions are recorded in an immutable ledger and all updates to that ledger are encoded in executable smart contracts, participants can not only execute the relevant smart contracts themselves to verify the update is valid, but they can cryptographically prove any incorrect or malicious behavior by the operators of the ledgers in order to make corrections or for use in any legal disputes.

This model eliminates some of the operational dependencies and inefficiencies of consensus based approaches in cases where there already exists an authoritative entity such as a central bank, central securities depository, clearing house or central counterparty. However, in markets in which there is no central governing entity or for purely bilateral use cases, certain entities would have to play the role of the operator(s) and interoperability between ledgers potentially becomes more important.

It should also be noted that regardless of the data integrity synchronization model, distributed ledgers are most secure when the asset being represented exists on-ledger in purely digital form. An example of this is dematerialized securities, the representation of which can exist purely in cryptographic form, and hence the ownership and transfer is governed directly by the ledger. However, DLT can also be used to represent assets that exist off-ledger, such as obligations to instruct a traditional system to make a payment or a physical good, such as gold. Physical goods clearly still require custodianship, which maintains the risk of theft or fraud, and their movement cannot be cryptographically guaranteed. Further, the process of porting an existing asset into an on-ledger asset, such as onboarding a paper certificate to cryptographic representation, is potentially subject to fraud and is a practical challenge that must be considered.

4.7 Smart Contract Security

The techniques described above are used by DLT to ensure data integrity and guaranty that all parties to the ledger share a single source of truth - a shared state. However, simply ensuring that there is shared state is not enough; there needs to be a common way to update a distributed ledger such that all nodes of the ledger continue to agree on an identical state of the ledger after processing all updates. The shared segments of code that carry out state changes on the ledger are typically referred to as smart contracts, and the accuracy of the state of the ledger is largely determined by the accuracy of the smart contracts. Essentially, the burden of correctness is pushed up from the distributed ledger to the smart contract - the integrity of a distributed ledger will be brought into question if there is no faith in the veracity of the contracts, which makes a discussion of smart contract language properties extremely important.

Smart contract languages and execution environments must ensure determinism of every supported operation. Determinism means that any two nodes processing a transaction will arrive at the exact same state. For example, many programming languages allow actions which are dependent on the time of processing; if such functionality were allowed in a smart contract language and two nodes processed a transaction at different times, they could have divergent views of the ledger. While determinism sounds like a simple property to evaluate, in practice building complex deterministic systems is not easy. For example, Bitcoin suffered multiple non-determinism bugs despite a very limited and simple contract language. There is a tradeoff between the flexibility of a more general language and the complexity of the execution environment. In evaluating a smart contract language, it is important to evaluate on both of these fronts.

In addition to determinism, many financial transactions require atomicity. An atomic transaction is an indivisible and irreducible series of operations such that either all occur, or nothing occurs. All distributed ledger technologies support some notions of atomicity, but many standard financial transactions - such as securities processing, which includes the simultaneous movement of two classes of assets (most commonly a security and cash) and operations such as netting and settlement which can involve atomic operations on millions of securities - are difficult to process atomically in most environments. When evaluating smart contract languages, and the execution environments for these languages, understanding the use cases to be implemented is critical to ensure that they can be handled deterministically.

Another aspect on which smart contract languages should be evaluated is built-in support for secure coding practices. Mission critical code needs to be written in languages and frameworks which have strong type checking, built-in tools to analyze for common mistakes such as integer overflows, built-in testing capabilities and facilities that abstract away complex tasks such as cryptographic operations.

Finally, the security of smart contracts can be enhanced if it is possible to statically analyze all possible future states of a contract, which reduces the likelihood of programmer error. Although many smart contract languages are derived from general purpose programming languages to allow for great flexibility in the hands of the developer using the language, this flexibility comes at a cost to analyzability. Smart contract languages that are domain specific to financial contracts tend to be more analyzable and therefore less prone to mismatches between the business intent and the code implementation. Examples of domain specific smart contract languages are DAML (developed by Digital Asset), Solidity, Ivy/Yvylang etc.

4.8 Digital Identity Keys

Identity is a critical area which is key to access control. Without a common understanding and agreed implementation of identity, data confidentiality and data integrity is vulnerable to mistakes or malicious behavior. This includes the need for a hierarchy relationship model – where entities with any form of affiliation are clearly linked – and the ability to delegate certain actions to other entities to act on your behalf to support common market structures. Furthermore, it is likely that some entities will be granted the authority to have custody of and manage their client’s cryptographic keys. For example, a custodian may also act on behalf of another custodian or an investor or investment fund, either signing on their behalf directly or having certain rights delegated to them.

One example of a platform independent implementation of identity management for DLT systems is Hyperledger Indy. The goal of Indy is to decouple identity from the DLT implementation so that the owners have a greater degree of control over its use and disclosure, sometimes referred to as “self-sovereign identity”. Indy has three key features to accomplish privacy in the design of its architecture: prevention of correlation with unique and pseudonymous identifiers, identifying information follows the off-chain confidentiality model with peer-to-peer encrypted connections and on-chain evidences, and additional support for zero-knowledge proofs. Indy’s model is similar to “web-of-trust” style architecture for identity and reputation management and is an open standard already implemented on multiple platforms. Decentralized Identifiers (DIDs) on the ledger point to DID Descriptor Objects (DDOs), signed JSON objects that can contain public keys and service endpoints for a given identifier.

4.9 Disaster Recovery (DR) and Back-Ups

A key disaster recovery challenge in any distributed (or even monolithic) system is the replication of data and the determination if the replica is accurate, and if not, where the loss of data or integrity lies. Fortunately, the same capabilities that enable DLT to offer improved business processes (distribution, integrity, monitoring and validation) provide benefits to support better DR capabilities.

High availability and DR are ‘free’ by-products of the fundamental distributed ledger architecture. Replicating systems and data for DR is hard for the reasons above and more. A better solution is to have always working replicas, geographically distributed, so that business can continue working in the event of outages elsewhere. DLT can avoid complicated storage or database replication techniques, replacing them with any number of distributed replicas. The distributed nature of the system implies that each node has a copy of the ledger or several nodes together have a subset. Monitors that look for integrity violations can determine if replicas are authentic and correct. If, during recovery, there is an invalid state in the system, i.e., because of replication error or as a result of the DR event, recovery is a challenge because special tools and procedures are needed to rebuild the data. A DLT maintains an immutable log of all changes and events. Recovery is easier because the system is always in a valid state otherwise the integrity validation processes would discover and report on any inconsistencies all the time, not just during particular DR events.

Having said this, entities should not rely purely on the distributed state of the system across their counterparties and continue to follow the best practices of DR as in today’s infrastructure.

4.10 Conclusion

Permissioned distributed ledger technology can be seen as an additional layer of security over existing systems today. The properties of DLT systems allow for increased data integrity, sometimes at the cost of confidentiality, and the primary benefits arise from this shared state rather than the increased levels of security. As with all networks, vulnerabilities still exist at the edges and the importance of securing private keys remains paramount. Before considering a certain solution over another, entities should ensure that sufficient external security audits have been conducted by qualified third parties.

There are several key considerations to take into account when selecting a DLT platform for use in financial services:

- The data confidentiality model must be performant, allow for continuous execution of processes, and not compromise the integrity of the overall network state.
- Whether sensitive data is stored on-chain or off-chain has major implications for information security.
- Segregating data onto separate networks for the purposes of confidentiality introduce similar issues with data silos as exist today.
- The use of encryption for maintaining sensitive data is subject to graph analysis to reveal sensitive information and increases the attack surface for malicious actors.
- Zero-knowledge proofs are an interesting but insufficiently tested cryptographic technique that potentially introduces highly complex security vulnerabilities.
- There is a convergence of platform designs towards the use of the insertion of fingerprints onto a blockchain with private data being shared point to point.
- Requiring all parties to sign transactions at the point of time that they are committed introduces new security and operational risks.
- Entities should carefully consider the need for a consensus algorithm if there is a natural entity that already acts as the authority for a ledger.
- If a consensus algorithm is required, there are many trade-offs to consider between approaches in this young but rapidly evolving field.

- Post-commit validation approaches may be more suitable for financial services, but perhaps only in circumstances in which there is already an authoritative party to leverage.
- The integrity of the ledger cannot be relied upon if security and integrity of smart contracts are compromised.
- The language employed for smart contracts has major security implications for multi-party financial workflows. General purpose programming languages may not be well suited to this new domain.
- Access control depends on the quality and security of digital identity, and keys must be protected from outside exposure.
- Identity systems should support the delegation of responsibilities to third parties in order to match the market structures that exist today.
- DLT is not a replacement for current DR approaches but may provide some additional properties that make recovery simpler.

A detailed discussion of consensus protocols and fault tolerance is contained in Appendix 3 "Information Security".

Appendices

Appendix 1

Review of Existing ISSA Principles

1. Introduction

The aim of this Appendix is to provide some analysis of the potential impacts DLT may have on ISSA's previous work. ISSA's previous document output can be divided into two categories. On the one hand there are the normative elements of ISSA's work, those papers that provide best practices or principles that ISSA encourages market participants to adopt. On the other hand a range of other ISSA publications exist which are descriptive in nature, outlining how various elements of securities services function or functioned at the time of writing.

This section focuses primarily on the former, normative category of ISSA's work. In particular, the documents used to conduct the review were:

- *ISSA Financial Crime Compliance Principles for Securities Custody and Settlement*
- *Final Report on Global Principles for Corporate Actions Processing and Proxy Voting*
- *Best Practices of Collateral Management for Cleared and Bi-laterally Traded Products*
- *Summary and Guiding Principles on European fund processing*

Reference was also made to ISSA's previous work on principles for OTC derivatives and to the work in particular of ISDA in this field.

The working group recommends to re-visit the ISSA document "Inherent Risks within the Global Custody Chain" at a later stage and to provide a more in-depth review of it.

Below, the impacts seen for DLT on ISSA's principles are condensed into a number of thematic categories. The aim is to establish the key factors in the nature of DLT that would lead to impact on principles and best practices published by ISSA. This can thus be used as a proxy for the effect on the securities servicing industry.

Following on from this, the report examines other considerations for specific elements of DLT implementations that would potentially impact ISSA principles.

Finally, the appendix section provides a detailed analysis of the existing ISSA principles against 3 different potential models for DLT implementation.

The principles put forward by ISSA concentrate on discrete topics or processes, such as the prevention of financial crime, the processing of corporate actions and investment funds, or best practices in collateral management. As such, they provide deep analysis of specific industry topics rather than broad comprehensive analysis of all aspects of the post-trade securities landscape. Broad analyses do however exist elsewhere, such as in the September 2017 publication from the ECB's Advisory Group on Market Infrastructures for Securities and Collateral[2].

With regard to the descriptive elements of ISSA's previous output, these are not part of the present analysis in detail. The reason for this omission is that, as descriptions of current actual market practice, these documents are likely best updated as concrete production-ready DLT systems come into existence. At the present juncture, such systems are not in place. An exception is made for ISSA's recently published Inherent Risks within the Global Custody Chain, where some high level analysis is provided in the appendix.

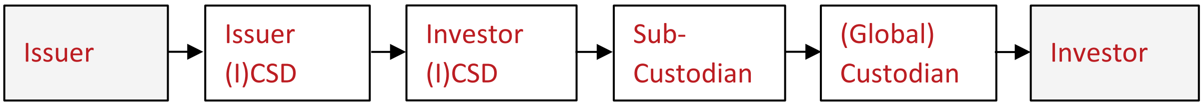
[2] The potential impact of DLTs on securities post-trading harmonization and on the wider EU financial market integration, AMI-SeCo, September 2017

2. Impacts of DLT on ISSA Principles

2.1 Participation on the DLT and Implications for Omnibus Accounts

The principles refer to information transfer between a range of intermediaries, normally custodian banks and (I)CSDs, that exist in the current market in order to pass information from the issuer to the investor.

Example:



Entities in this chain should maintain an electronic STP flow of information from issuer to investor and vice versa. How much of this current process outlined above would be affected by the introduction of a DLT-based system will depend on the scope and membership of that system. At its most extreme, assuming that the DLT solution features all issuers and all end investors, this may imply a direct non-intermediated connection with the end investors.

In such a circumstance, the concept of omnibus accounts, where the assets of multiple beneficial owners are commingled, becomes unnecessary. ISSA principles focusing on omnibus accounts therefore would also become redundant. Direct participation of issuers and end investors also renders obsolete the necessity to pass information through a custody chain; thus principles relating to the transmission of information through a chain of intermediaries would also become less relevant in such an implementation.

It is worth noting that this is not the sole participation model possible via DLT systems. Some intermediation may still be needed depending on the entities participating on the DLT network, especially should omnibus positions be a reality on the ledger.

2.2 Reconciliation

DLT implies the distribution of a ledger between multiple participants. In a permissioned system, either the ledger will be distributed to all participants, but records will be obfuscated to only show those relevant to a specific participant, or a hierarchy can be introduced where validator nodes maintain complete copies of the ledger while participants only maintain sections of the ledger relevant to them. Depending on the membership of the DLT system, this will reduce or remove the need to reconcile holdings between participants. Principles targeted at reconciling holdings between counterparties would therefore become unnecessary if the counterparties were both participants of the DLT system.

3 Other Considerations

3.1 Functions Covered by the DLT

ISSA principles are targeted at systems providing the following functionalities:

- Identification of participants / beneficial owners
- Custody of cash and / or securities assets
- Transmission of transactions (settlement) of cash (in either CeBM or CoBM) and / or securities
- Storage and access of reference data concerning securities and their issuers

- Messaging systems to transmit information and voting or corporate action election instructions between issuers and investors and vice versa.

A DLT implementation may cover all or a subset of these functionalities. The scope of the DLT's functionalities will naturally affect the impact it has on ISSA principles covering the above topics. (For example, a DLT system that functions purely as a messaging service for Corporate Actions will have a more limited impact on ISSA principles than a DLT system providing DVP settlement in central bank money along with full two way corporate actions transaction services).

3.2 Geographical Scope of the DLT

Some of the first permissionless DLT systems introduced were envisaged as being global in reach. That being said, the first examples of DLT implementations for securities services will have more limited geographical scope.[3] Should this trend continue and the early DLT implementations continue to be broadly national in character, the impact on current market structure, and thus ISSA guidance, is likely to be limited in the short to medium term. This is because cross border holdings would still necessitate the intermediated holding structures we are familiar with today.

If, on the other hand, the scope of services provided by the DLT has wider or global geographical coverage, ISSA guidance is likely to be more affected. Such DLT implementations would have to cover multiple divergent market practices, which may increase the complexity of the platforms.

Furthermore, ISSA does not envision that there will be only one DLT platform going forward. It is very likely that separate DLT implementations will develop organically in divergent geographies. This in turn will necessitate a strong focus on interoperability solutions once DLT use cases move into production. ISSA understands that interoperability standards are being developed, but are likely only to become a high priority once base technical standards for permissioned DLT systems are fully developed. As mentioned in section 3.5 "Business Standards and Integration" (in the main report), the financial industry is currently using commonly agreed business standards such as ISO 20022, and these, or potentially a more suitable standard accomplishing the same objectives should therefore be re-used in a DLT context.

3.3 Settlement Schedules

Current processes define a difference in timing between when a trade is carried out and when the settlement of the securities versus cash of that trade takes place. In the EU, the US and many other jurisdictions, this time gap is two business days, referred to as T+2. This gap exists primarily as a result of market practice, including practices in pure cash markets and foreign exchange markets.

Under a DLT solution, it is theoretically possible for settlement to occur at a range of user-defined intervals between T+X and T+instant (i.e. the duration between the trade and the settlement could be more flexibly determined by the counterparties). More flexible settlement cycles, or indeed instant settlement, would have implications for market liquidity and for a variety of processes which ISSA provides guidance on through its principles; for example, it may have impact on collateral management practices, or the timing of voting on corporate actions.

Similarly, depending on the geographical coverage of the network, instant settlement in tandem with multiple time zones represented on the ledger may bring about new issues on which ISSA may be required to provide guidance.

[3] For example ASX is implementing a DLT-based system, planned for Q42020/Q12021, as a replacement for its CHESS system.

3.4 Interaction of the DLT with other Elements of the Trading and Post-Trade Landscape

A DLT implementation may have impact on processes upstream from or downstream to custody and settlement. Examples of such impacts could include:

- The role of a CCP may change depending on the nature of the DLT. In a T+instant environment for cash securities including equities and fixed income instruments, counterparty risk on settlement between participants would be eliminated, thus removing the need for novation and risk management via a CCP to reduce and manage counterparty risk. However, with regard to derivatives transactions, CCPs will continue to play an important risk management role, due in part to the large passage of time between the commencement and conclusion of a derivatives contract. It is also possible that a DLT based system could make use of a central counterparty system for the purposes of multilateral netting and the ensuing reduction in liquidity needs.
- Corporate action and proxy voting processes could change if both issuer and end beneficial owner were represented on the DLT network. For example, direct issuer-inputted information on the network would obviate the current need for the collection of corporate event information from multiple sources to create a "golden copy" of a corporate event, and would also simplify or eliminate the process of intermediation of this information (and transactions / elections resulting from it) through a custody chain.

Examples above are by no means exhaustive, and there may be additional spillover impacts on other areas of securities services possible dependent on the specific DLT implementation under discussion.

3.5 Business Logic within the DLT

While not necessarily part of a DLT implementation, in-built business logic opportunities, presented through either chain code or smart contracts (refer to the information security section), allow for processes conducted based on trusted third party arrangements today to become automated and embedded in a DLT. For example, today, ISSA principles stipulate that a custodian should communicate KYC standards and other compliance and risk-based requirements to their account holders, which then the account holders are required to follow. In a DLT system using smart contracts, potentially KYC standards and other requirements could be embedded directly into the ledger, making deviation from the encoded standard very difficult.

The scope and extent to which such systems are used will therefore have an impact on ISSA guidance in a wide variety of areas.

3.6 Crypto Assets [4]

The nature of the asset being transacted via the DLT may have an impact on ISSA guidance. Currently, it appears two separate classes of assets can be distinguished in this respect:

- Tokens on the DLT that represent assets not held on the ledger. Examples of such tokenized representations can cover everything from real estate, high value physical assets to tokenized securities or cash.
- "Digital native": these are assets held on the DLT with no reference to assets held outside of the DLT.

Other considerations can distinguish different forms of "digital native" assets, including the nature of the issuing entity, the process of issuance, and the purpose of the asset.

[4] This topic will be explored further in future ISSA publications.

In summary, the nature of the asset and the regulatory framework under which it operates may have significant and wide ranging impacts on ISSA guidance, in particular should the assets held on the DLT be considered comparable to securities.[5]

4 Conclusions

The result of the ISSA analysis is that DLT is a malleable technology and its impact is very much dependent on the specific deployment envisaged. Moreover, ISSA principles are by and large technology agnostic, focusing primarily on providing recommendations on business processes, interactions between various securities services actors and market governance.

Based on this, ISSA draws two conclusions on the potential impact of DLT on its previously published principles:

- At one end of the spectrum, DLT implementations can imply little to no impacts on current ISSA principles, as the structures, governance and market practices under which current markets operate can be transposed to DLT-based infrastructures. In the short term, ISSA believes the majority of DLT use cases coming into production situations are likely to mirror current market practices to a large extent, and therefore will not represent a major break with current ISSA principles.
- At the other end, it is clear that DLT can however be used to fundamentally transform roles and processes in the securities services landscape and potentially tie issuers of securities directly to all their investors, eliminating frictions. Here, transformation arises not only on the basis of technological change, but also changes of other factors, including market practices, regulation and so on. ISSA believes such changes will only happen in the longer term as DLT as a technological basis becomes more mainstream and market structures are adjusted to leverage the technology further.

5 Suggested Next Steps

Production-ready DLT implementations in the securities services space currently are not in place, and early exemplars of production systems that are currently under development are likely to closely mirror established financial market structures. In the immediate future therefore, the impact of DLT on ISSA guidance will likely be minimal.

Having said this, it is clear that the technology could have significant impact on the roles, shape and practices in the post-trade area. The above analysis, together with the detailed review provided in the appendix, form an initial basis and framework for assessing the impact on ISSA's normative work from a theoretical perspective. Going forward, as concrete use cases will develop, these elements can also serve as a basis when assessing their impact on current processes.

The working group furthermore recommends this work be reviewed and developed once a number of concrete DLT implementations have taken place. In particular, it is at this later stage that a more in depth review of the more descriptive elements of ISSA's work, notably encapsulated in the document *Inherent Risks within the Global Custody Chain*, will be called for.

[5] The scope of purposes for crypto assets is wider than traditional securities, including such functions as:
- a means of exchange (a "crypto currency");
- a representation of rights of the holder in an organization ("crypto equity");
- a claim on future profit or income ("crypto investment");
- an element used to interact with / use a service (a "crypto resource")
- an asset to be owned in its own right (a "crypto commodity")

6 Detailed Analysis of ISSA's Normative Principles

6.1 Outline of the Models Used to Assess Impact on ISSA's Normative Principles

Below is a more detailed analysis of ISSA's normative principles against three different models for how a DLT system could be implemented. These models are loosely based on analysis by the European Central Bank in 2016.[6]

The models below are organized to represent increasing levels of disruption from the status quo. The reader should additionally note that they are designed to represent points in a spectrum of possible DLT applications rather than comprehensively referring to all possible DLT implementations. As such, while presented as discrete in the below analysis, the reader should note that other intermediary models between those described below could also come into being.

The work below therefore could potentially be updated at a future date once production-ready DLT systems come into being and provide a more concrete basis for further analysis.

Also included separately is the role smart contracts could play. This is provided as a discrete item given the fact that DLT systems can be envisaged with or without integrated business logic code.

6.2 Model 1 – Intermediated DLT

Incumbent institutions make use of DLT to improve either their internal efficiency or the efficiency between groups of similar organisations. Under this model, existing business arrangements would be replaced by an equivalent system composed of DLT implementations, without significant impact on the institutions themselves.

"CSD-like" DLTs would develop independently over different geographies, with participation in these systems being limited to small numbers of custodian entities. These entities in turn may provide DLT systems to their customers or systems based on other, potentially legacy, technology. Interledger standards or protocols, along with interfaces to SWIFT messaging would be crucial to ensuring interoperability in this model.

A difference is retained in this model between trade cycles, clearing cycles and settlement cycles.

6.3 Model 2 – "Issuer CSD" DLT

CSDs adopt market-wide distributed ledgers with broader participation. In this model we assume securities-holding persons, both legal and natural, would have wallets directly on the DLT, with a "CSD-like" entity acting as gatekeeper providing access to the system to individuals and entities following a KYC process.

With direct access to the DLT, the need for intermediated custodial functions becomes unnecessary, as does potentially the need for omnibus accounts commingling the securities of multiple participants.

This model is still construed as primarily providing post-trade rather than functions in the trading layer.

[6] ECB Occasional Paper Series No. 172 / April 2016, https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf

6.4 Model 3 – “Peer to Peer” Network

Here we assume that issuers and investors take the lead in implementing a peer to peer system based on DLT, with potentially a trade venue providing exchange functions between participants.

In this scenario, again, no intermediated access to settlement infrastructure is necessary, with a difference with model 2 being that here trading and settlement become the same process.

We could envisage in this model either the Trading Venue providing a gatekeeper role providing access to the system, or alternatively it may be the case in this model that no gatekeeper model exists.

6.5 Financial Crime Compliance Principles for Securities Custody and Settlement

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
1	It is the responsibility of the custodian to communicate to its account holders any relevant Know Your Customer ("KYC") standards and other compliance and risk-based requirements that it expects them to follow.	**No impact**	**Impacted** In this model we would envisage that the Issuer CSD entity would be responsible for communicating these details to their account holders rather than a custodian entity.	**Impacted** Depending on the nature of the DLT, this role would either have to be taken on by the trading venue for the DLT, or may not functionally be possible if no "gatekeeper" role is envisaged.	Smart contracts or chain code could potentially be used to embed such rules in the DLT system, making compliance virtually mandatory. There would likely still be a need for a KYC / onboarding function to act as gatekeeper to the DLT irrespective of model.
2	It is the responsibility of the account holder to comply with those standards and requirements.	**No impact**	**No impact**	**No impact**	Compliance may be made mandatory through smart contract logic identifying the scope of actions a particular participant could conduct.
3	Where the account holder has direct clients who themselves accept deposits of third party client securities, it is the responsibility of the account holder to notify the clients that by holding securities cross-border they will be subject to the requirements of the jurisdictions in which the securities entitlements are held, including the standards of the relevant custodian(s).	**No impact**	**Impacted** In this model the scope for intermediated holding structures is reduced; as such the need for transmission of information concerning jurisdictional rules along an intermediary chain may not be necessary. Likely the issuer CSD entity would take on the role of communicating the rules governing the DLT directly to all DLT participants.	**Impacted** In this model, no intermediation is envisaged, removing the need for information concerning jurisdictional rules to be passed through a chain or parties. It may fall to the trade venue to perform the function of informing the participants about such rules, or alternatively there may be no party responsible for conducting this function.	The same commentary applies here as with principle number 1.

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
4	It is the responsibility of the account holder to sub-deposit securities with the custodian only when the Ultimate Asset Owners have been subjected to satisfactory due diligence. If the Ultimate Asset Owners of the securities are not themselves directly client of the account holder, then it is the responsibility of the account holder to ensure that its direct client have undertaken the appropriate level of due diligence. On a risk-led basis, the custodian should be entitled to verify that its due diligence standards have been met. Third party agents or reports may be relied upon for this purpose	**No impact** KYC and due diligence procedures would likely be conducted in a manner similar to today.	**Impacted** In this model, an issuer CSD entity would be acting as a gatekeeper to the network. This entity would likely be responsible for performing KYC and due diligence on all DLT participants, rather than delegating this responsibility through a chain of intermediated custodians.	**Impacted** In this model, the trade venue may provide this function, or, if no gatekeeper role is envisaged, it may not be possible for such procedures to be conducted.	Suitability control check could be provided within the smart contract rule set.
5	The custodian must ensure that all accounts are designated by the account holder as intended for the deposit of proprietary or client interests in securities. accounts designated as client accounts must be sub-classified as either segregated, holding securities for one single client of the account holder or omnibus, commingling securities belonging to or held for several clients of the account holder.	**No impact**	**Impacted** Accounts on the ledger would be proprietary accounts only, rather than holding assets on behalf of a third party. Descriptions concerning the usage envisaged by the party being granted access to the ledger would likely form part of the initial approval process granting access.	**Impacted** Accounts on the ledger would be proprietary accounts only, rather than holding assets on behalf of a third party.	Suitability control check could be provided within the smart contract rule set.
6	Non-proprietary segregated accounts may be held only by account holders authorized to accept client assets and monies that have adequate compliance and control functions fulfilling the demands of safekeeping client assets.	**No impact**	**Impacted** The same considerations apply as with principle 5.	**Impacted** The same considerations apply as with principle 5.	The same considerations apply as with principle 5.

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
7	When an account holder opens a segregated account for a third party with the custodian, the account must be associated with the name of that third party.	**No impact**	**Impacted** The same considerations apply as with principle 5.	**Impacted** The same considerations apply as with principle 5.	
8	In addition to the provision of Principle 7 above, the account holder must declare to the custodian the ultimate asset ownership of the assets deposited on a segregated account holder's account. An exception to this is when the segregated account holder's account is maintained on behalf of an underlying client itself depositing securities with the account holder on an omnibus basis. In such a case the custodian should apply, to the account holder, the principles that govern the maintenance of omnibus client accounts (Principles 9 and following).	**No impact**	**Impacted** The same considerations apply as with principle 5.	**Impacted** The same considerations apply as with principle 5.	

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
9	Omnibus client accounts commingling securities held for several client of the account holder may be opened and maintained only by those account holders that: ▪ Are regulated and authorized to accept client assets and monies; Have compliance and control functions reasonably designed to ensure compliance with client asset protection rules or, in the limited case of third countries that do not regulate safekeeping, have appropriate policies and procedures in place; ▪ Represent that they have applied any specific requirements communicated by the custodian to the business of the client of the account holder whose securities are sub-deposited with the custodian and can demonstrate that reasonable steps are taken to verify compliance; ▪ Screen transactions and holdings against lists of designated persons under sanctions and other relevant programs consistent with any requirements communicated by the custodian.	**No impact**	**Impacted** The same considerations apply as with principle 5.	**Impacted** The same considerations apply as with principle 5.	
10	In case the account holder opens an omnibus client account with the custodian, it must disclose to the custodian the geography, segments and products which the omnibus client account supports.	**No impact**	**Impacted** The same considerations apply as with principle 5.	**Impacted** The same considerations apply as with principle 5.	

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
11	In considering whether to open an omnibus client account for an account holder, the custodian should evaluate the risk factors present, including the reputation and jurisdiction of the account holder, the geographies, segments and products that the account is intended to support and the nature of the account holder's activity.	**No impact**	**Impacted** The same considerations apply as with principle 5.	**Impacted** The same considerations apply as with principle 5.	
12	The account holder must inform the custodian promptly of any intention to materially change its use of the omnibus client account. The custodian reserves the right to decline the use of the omnibus account to support any new business activity of the account holder.	**No impact**	**Impacted** The same considerations apply as with principle 5.	**Impacted** The same considerations apply as with principle 5.	
13	The custodian has the right to conduct activities to verify its account holder's compliance with the requirements including requesting that the ultimate asset ownership of assets deposited on omnibus client accounts be disclosed to the custodian via an agreed operational procedure based on predicated risk factors (i.e. red flags). The beneficial ownership of assets deposited on omnibus client accounts shall be disclosed to the custodian in case of an enquiry by a regulatory authority, judicial authority or the issuer of those assets provided there is sufficient legal basis (as determined by the custodian) to justify the request.	**No impact**	**Impacted** These rights would likely be maintained by the Issuer CSD entity acting as gatekeeper, who would have direct knowledge of the beneficial ownership of assets being deposited in accounts, since all accounts would be operating on a proprietary basis.	**Impacted** These rights may be maintained by the trading venue, or if no gatekeeper role is involved it may not be possible for one party to conduct the processes described. Again here, we should note that accounts on the DLT implementation on this model would be operating on a proprietary basis only.	

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
14	In the case of an omnibus client account where clients of the account holder have themselves deposited securities in this account on an omnibus basis, the custodian should: ▪ Require its account holder to apply the standards to its client that the custodian requires; ▪ Be entitled to require that its account holder is in a position to identify the Ultimate Asset Owners of the assets deposited and to disclose those identities in accordance with Principle 17; ▪ Require that its account holder performs due diligence to ensure that its client meet the requirements of Principles 9 – 16.	**No impact**	**Impacted** The same considerations apply as with principle 5.	**Impacted** The same considerations apply as with principle 5.	

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
15	The account holder which has opened an omnibus client account with the custodian must ensure that it has an appropriate level of visibility over the business of its branches, subsidiaries, business divisions and affiliates that are entitled to also use this omnibus account.	**No impact**	**Unclear** This depends on whether individual branches, subsidiaries and business divisions would be maintaining separate accounts on the DLT, or whether this activity is pooled into one account maintained by the parent legal entity. In the former circumstance, this principle may not be necessary as such visibility is provided by the fact that these individual branches, subsidiaries and so on are direct participants in the DLT. In the latter circumstance, this principle would still apply and the issuer CSD would need a way of ensuring that the parent legal entity could maintain such visibility. Legal entity identifiers (LEIs) may play a role here.	**Unclear** This depends on whether individual branches, subsidiaries and business divisions would be maintaining separate accounts on the DLT, or whether this activity is pooled into one account maintained by the parent legal entity. In the former circumstance, this principle may not be necessary as such visibility is provided by the fact that these individual branches, subsidiaries and so on are direct participants in the DLT. In the latter circumstance, this principle would still apply and the trade venue, if acting as a gatekeeper to participation on the DLT, would need a way of ensuring that the parent legal entity could maintain such visibility. Legal entity identifiers (LEIs) may play a role here. If the trade venue does not act as a gatekeeper to participation, it may not be possible for this principle to be fulfilled.	

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
16	The custodian should undertake periodic reviews on a risk basis of its account holders which have opened an omnibus client account to ensure that these requirements are continuously observed.	**No impact**	**Impacted** It would likely be the Issuer CSD conducting such reviews on DLT participants operating on the network for proprietary business.	**Impacted** If the trade venue acts as a gatekeeper to participation, this entity would likely conduct such reviews on its participants on their proprietary activity on the network. If no gatekeeper role is envisaged, there may be no party able to conduct such reviews.	
17	The custodian should be entitled to require its account holder to disclose the identities of the ultimate buyer and/or seller of a security in response to a specific request predicated on risk factors (i.e. red flags) within a reasonable period. Where the client of the account holder is itself an intermediary, the custodian should be required to ask its account holder to have its client(s) disclose the identities of the ultimate buyer, seller and/or other related parties and to communicate the data to the custodian within a reasonable period of time.	**No impact**	**Impacted** The issuer CSD would have direct knowledge of the participants in the network.	**Impacted** If the trade venue acts as a gatekeeper to access to the DLT, it would have direct knowledge of participating entities. If the trade venue does not provide this function, there may be no centralized party able to require such disclosures.	Controlled by smart contracts

6.6 Collateral Management

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
1	Wherever possible, standardized industry legal documentation should be used to support a collateral agreement between a collateral provider and a collateral taker.	**Not impacted** With the introduction of DLT, no change to the need for standardized industry legal contracts between parties.			
2	The collateral provider and the collateral taker must agree on the type of collateral arrangement they execute and have a shared understanding of «who owns what».	**Not impacted** With the introduction of DLT, no change to the need between parties to agree on the type of collateral arrangement (pledge vs. transfer of title) and a common view of who owns what.			
3	All risk bearing and operational units within a firm should ensure that the standardized contract terms address their risk requirements	**Not impacted** With the introduction of DLT, no change of the need of all entity's risk requirements to be covered in the standardized contracts.			
4	Firms should adopt a flexible approach to rehypothecation and be prepared to support limits and enhanced reporting on its use.	**Not impacted**	**Impacted** The settlement timings may present additional challenges for rehypothecation (e.g. T+0 settlement may lead to greater levels of settlement failure as a result of rehypothecation)	**Impacted** In this model we envisage the trade and settlement operations taking place simultaneously, so as with model 2 there may be impacts as a result of T+0 settlement.	Smart contracts could provide greater levels of control on rehypothecation (e.g. by specifying the number of times a security can be rehypothecated and/or in which proportion).
5	Firms must always be cognizant of the relationship between the account structure and the agreement terms.	**Not impacted**	**Impacted** The account structures DLT actors may have could lead to divergence from current account-driven collateral management practices	**Impacted** The account structures DLT actors may have could lead to divergence from current account-driven collateral management practices	Smart contracts could include the agreement terms i.e. pledge vs. transfer of title

<table>
<tr><th colspan="2">Principle</th><th>Model 1</th><th>Model 2</th><th>Model 3</th><th>Potential for Smart Contracts</th></tr>
<tr><td>6</td><td>Firms should understand legal, commercial, credit and operational risk implications associated with the choice of a particular collateral.</td><td colspan="3"><b>Not impacted</b>
With the introduction of DLT, no change in the need to understand the legal, commercial, credit and operational risk implications associated with the choice of a particular collateral.
However, operational risk implications may of course be impacted by the model in question (for example with reference to custody arrangements on the ledger)</td><td></td></tr>
<tr><td>7</td><td>The collateral payer should have the choice of the bank / investment vehicle selected to hold its cash collateral and the determination if the account should be commingled or segregated.</td><td><b>Not impacted</b>
This may require cash to be held on the DLT</td><td><b>Impacted</b>
This would require cash to be held on the DLT. Accounts would likely be proprietary for such purposes, and may not involve commingling.</td><td><b>Impacted</b>
This would require cash to be held on the DLT. Accounts would be proprietary and would not involve commingling.</td><td></td></tr>
<tr><td>8</td><td>The collateral payer should have transparency over the collateral receiver's investment objectives for the cash collateral.</td><td colspan="3"><b>Not impacted</b>
With the introduction of DLT and assuming cash as collateral is covered, no change in the need for transparency in the collateral receiver’s investment objectives for the cash collateral.</td><td>The investment objectives could potentially form part of the smart contract governing the collateral movements, providing greater security in this respect.</td></tr>
<tr><td>9</td><td>A re-invested collateral portfolio should be valued on a daily basis with a mark-to-market process.</td><td colspan="3"><b>Not impacted</b></td><td></td></tr>
<tr><td>10</td><td>Counterparties should carefully review the credit, market and operational risks associated with the choice of non cash collateral.</td><td colspan="3"><b>Not impacted</b>
With the introduction of DLT, no change in the need to carefully review the credit, market and operational risks associated with the choice of non cash collateral.</td><td></td></tr>
</table>

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
11	Non cash collateral should be reconciled to its holding location and valued on a daily basis.	**Not impacted** Non-chain clients would still have to reconcile their holdings with on-chain participants. Valuation processes would likely not be impacted as this would be a separate collateral management function.	**Impacted** Records of holdings could be maintained by the DLT and accessible to participants without the need for reconciliation. Whether the need for reconciliation is completely removed would depend on whether the DLT provides sufficient granularity at the individual trade / exposure level of participants. Valuation processes would likely not be impacted as this would be a separate collateral management function.	**Impacted** Records of holdings could be maintained by the DLT and accessible to participants without the need for reconciliation. Whether the need for reconciliation is completely removed would depend on whether the DLT provides sufficient granularity at the individual trade/exposure level of participants. Valuation processes would likely not be impacted as this would be a separate collateral management function.	
12	As concerns UCITS, the collateral receiver (or taker) should carefully select the custodian of its collateral. When a UCITS receives the collateral under title transfer, it has to be held with the depositary. However, the depositary of the UCITS can sub-deposit these assets received as collateral to sub-custodians, such as banks and/or ICSDs (i.e. on triparty collateral accounts opened in the name of the depositary of the UCITS specifically for this purpose and this UCITS).	**Not impacted** Non-chain clients would still have to choose their custodian for UCITS fund units	**Impacted** Fund units would likely be held on proprietary participant accounts on the DLT rather than through an intermediated structure. Sub depositing would likely not be necessary.	**Impacted** Fund units would be held on proprietary participant accounts on the DLT rather than through an intermediated structure. Sub depositing would likely not be necessary.	

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
13	The collateral payer and service providers should at all times ensure that the payer is not over-collateralized with their trade counterparties.	**Not impacted** This would still apply although the movements may take place on the DLT.			Movements of collateral to rectify over/under-collateralization could potentially be automated via smart contracts.
14	Firms should consider expanding due diligence functions surrounding Independent Amount (IA)especially in light of recent regulatory reform.	**Not impacted** This relates to legal arrangements between parties rather than operational procedures involving collateral movements / settlement and custody functions.			
15	Firms should be prepared to accept a variety of IA arrangements.	**Not impacted**	**Impacted** The availability of the varying segregation models applied in the principle may not map to a DLT setting of proprietary accounts only.	**Impacted** The availability of the varying segregation models applied in the principle may not map to a DLT setting of proprietary accounts only.	The tagging of the asset of IA could potentially take place via smart contracts with limitations placed on what acceptable usage of such assets would consist of.
16	Attention should be given by the client to the choice of not only the clearing member(s) selected but also to the choice of the CCP(s) selected as they represent the ultimate risk for the client.	**Impacted** The role of a CCP may change depending on the nature of the DLT. In a T+instant environment, counterparty risk on settlement between participants would be eliminated, thus removing the need for novation via a CCP. However, with regard to derivatives transactions, we believe CCPs will continue to play an important collateralization role. In this context, we believe this principle still applies, with a CCP in this context likely being a ledger participant.			
17	Firms must be aware at all times of the segregation terms available.	**Not impacted** This would relate to the organizational arrangements connected to the CCP rather than to the DLT.			
18	Firms must understand each CCP's ability to port trades from a defaulting member's account to a non-defaulting member's account.	**Not impacted** This would relate to the organizational arrangements connected to the CCP rather than to the DLT.			

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
19	Firms must be aware of the discrete operating environments for each CCP.	**Not impacted** This would relate to the organizational arrangements connected to the CCP rather than to the DLT.			
20	Design MIS procedures to allow rapid data queries or reporting as required, including information on balances, exposure values, legal entity names, etc.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
21	Ensure appropriate account naming conventions and account structure for all collateral accounts.	**Impacted** Naming conventions on accounts for the participants would likely be replaced by conventions governing the public and private keys for the wallets on the DLT	**Impacted** Naming conventions on accounts for the participants would likely be replaced by conventions governing the public and private keys for the wallets on the DLT. It is questionable whether there would be separate “wallets” specifically for the purposes of collateral management	**Impacted** Naming conventions on accounts for the participants would likely be replaced by conventions governing the public and private keys for the wallets on the DLT. It is questionable whether there would be separate “wallets” specifically for the purposes of collateral management	Smart contracts could potentially be used to track assets being used as collateral, rather than this being determined by account structure.
22	Keep all agreements in a single location, ideally electronically, to easily download all executed documentation against a specified entity.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
23	Understand all legal documentation and implications of all clauses, particularly those pertaining to default or insolvency.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
24	Maintain a searchable database of agreements to capture non-standard terminology that could require exceptions or modifications to normal procedures in the event of a default.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
25	Know which entities to instruct in the event of a counterparty default (e.g. custodian, collateral agent, etc.).	**Not impacted**	**Impacted** Relationships in such circumstances may rather be direct between the defaulting party and the entity in question rather than via an intermediated custody structure.	**Impacted** Relationships in such circumstances may rather be direct between the defaulting party and the entity in question rather than via an intermediated custody structure.	
26	Create and regularly update a crisis event «playbook», which can include an overview of possible default scenarios and tactical steps required in the event of a default.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
27	Immediately access all relevant legal documentation to facilitate legal review.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
28	Generate and collate all necessary reporting to identify all exposures against the defaulting party, including collateral positions and value.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
29	Contact legal and compliance representatives to follow guidance related to the specific default scenario as actions are likely to vary.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
30	Follow the collateral liquidation process per legal guidance.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
31	Maintain a master list of legal entities that have declared bankruptcy, and associated dates of bankruptcy, to prevent confusion within the organization	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			
32	Provide transparency throughout the process to ensure key stakeholders are aware of necessary actions.	**Not impacted** This relates to internal organizational and operational procedures rather than to the movement of collateral via a DLT.			

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
33	Maintain constant communication with custodian and/or collateral agent. Legal agreements may call for a cease or change of day-to-day procedures for applicable entities, unless otherwise instructed by courts or trustees.	**Not impacted**	**Impacted** Relationships in such circumstances may rather be direct between the defaulting party and the entity in question rather than via an intermediated custody structure.	**Impacted** Relationships in such circumstances may rather be direct between the defaulting party and the entity in question rather than via an intermediated custody structure.	
34	Adoption of automated solutions for margin call issuance and response.	**Not impacted**			Smart contracts could potentially be used to automate margin calls on the DLT, although it remains to be seen whether this could solely occur on an individual transaction level or over the entirety of a portfolio.
35	Adoption of automated solutions for the pledge and release aspect of third party collateral movements.	**Not impacted**	**Impacted** Account structures may lead to this process being more bilateral than via a third party.	**Impacted** Account structures may lead to this process being more bilateral than via a third party.	Smart contracts could potentially be used to code have pledge and release logic into collateral operations on the DLT.
36	Automate solutions for standard and bespoke reporting.	**Not impacted** We assume the ledger would provide some form of interface or connectivity allowing for reporting. The design of the reporting would likely be an internal organizational consideration of the entity in question rather than something specifically related to the DLT.			
37	Adoption of automated solutions for reconciliation.	**Not impacted**	**Impacted** The level of reconciliation required may be reduced by the lower level of custodial intermediation.	**Impacted** The level of reconciliation required may be reduced or removed by the lower level of custodial intermediation.	

6.7 Corporate Actions

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
1	**Straight-Through Processing (STP) and ISO Standards** Communication should be electronic to ensure an STP flow along the intermediary chain from the issuer to the investor and vice versa. Messaging must be in ISO format and in structured standardized data form across the issuer to investor chain. In implementing ISO standards, local market practice will be adopted as defined by NMPGs (National Market Practice Groups), and ISO 'Extensions' adopted if agreed local market practice cannot be accommodated within the existing global standard and harmonized global market practice.	**Impacted** Firstly, the scope of the DLT is important – considerations will be different if it is only being used as a system for the transfer of information related to corporate actions, or if it also involves the movement of assets such as cash and securities on the ledger. In the former case, we note that an ISO standard does not currently exist for communication via Distributed Ledgers (but the ISO 20022 business elements should be re-used). We also note that this would entail a split between the current situation where messages are transmitted between parties based on custody positions. In the latter case this link could still be maintained although complexity could be created by using the same system to record transfers of assets and transfers of information about corporate events. We also note that in the present day this principle is not completely observed in the sense that transmission of information to end beneficial owners (natural persons) is still in some jurisdictions and companies conducted via paper mail rather than electronic communications.	**Impacted** In addition to the considerations for model 1, in this model the scope of intermediation is greatly reduced. It is possible that instead of information being passed along a chain of intermediaries, investors have more or less direct access to the information provided by the issuer.	**Impacted** In addition to the considerations for model 1, in this model the scope of intermediation is greatly reduced. It is possible that instead of information being passed along a chain of intermediaries, investors have more or less direct access to the information provided by the issuer.	

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
2	**Message Content** The content of messages must be clear, contain all known key information and be unambiguous. In particular, all key dates and critical information affecting an event must be carried in the event announcement, including a record date for elective events that is prior to the election deadline.	**Impacted** The considerations mentioned above for principle 1 would also carry over here.			
3	**Issuer Sourced Key Information** Key summary information must be created by the issuer. It should be, at a minimum, consumable and accessible using the ISO repository of data elements and subsequently usable in structured ISO format and should be simultaneously published to the local exchange and CSDs, regulators and the open market. Issuers should also make prospectus documents (e.g. event terms and conditions) available on public websites. Updates should contain all known information, as a best practice, and recipients should manage any discrepancies from previous messages.	**Not impacted** The responsibilities of issuers to provide the information described in this principle remains.			
4	**Required Information** Subject to compliance with legal requirements, only information that is required for the event type should be carried in the announcement, i.e. only data functionally necessary for processing in an electronic, structured way, as defined by designated organization(s) in each market, implementing standards consistent with global ISO standards. This information must be unambiguous. Other optional information should be retained and accessible at source.	**Impacted** The considerations outlined for principle 1 may also apply here. The general goal of this principle to only transmit required information would carry through to a DLT setup.			

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
5	**Unique Identifiers** Required information must include a unique global event identifier that is assigned at the earliest possible point and remains with the event throughout its lifecycle, despite up-dates. Issuer and security codes should uniquely identify the issuer as well as the listing location, e.g. using ISIN and MIC.	**Impacted** This role may in fact become more important if there is a separation between custody positions and the transmission of corporate event data. Currently each organization in the custody chain may apply its own identifier; in a DLT setup it may be more necessary to apply a single identifier to the corporate action.			
6	**Timelines of Notification** Notifications and updates to the chain of intermediaries and to the end investor must be made in a timely manner and as close as possible to the issuer's announcement date and time. Sufficient notice to execute the event, including amendments to the event, must be given to allow all parties to complete the process effectively before the event deadline.	**No impact**	**Impacted** Intermediation chains are likely to be significantly reduced or removed in this model, thus making instruction deadlines closer to the true issuer event deadline. If the DLT serves the sole purpose of transmission of corporate event data, this could also lead to advantages with the version of the event on the ledger forming a golden copy able to be transmitted to all participants directly on the ledger, again reducing the need for intermediation here.	**Impacted** Intermediation chains are likely to be significantly reduced or removed in this model, thus making instruction deadlines closer to the true issuer event deadline. If the DLT serves the sole purpose of transmission of corporate event data, this could also lead to advantages with the version of the event on the ledger forming a golden copy able to be transmitted to all participants directly on the ledger, again reducing the need for intermediation here.	

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
7	**Process Harmonization** Where global or regional standards do not already exist, each market should agree its standards for corporate actions processing and, in parallel, aim at convergence of standards across markets. Processing should involve book-entry payments for both cash and securities proceeds. Standard election option identification conventions should be adopted to facilitate the election process. Clear rules should be published by markets on the processing of reversals, which should be pre-advised in all cases and should require the prior consent of intermediaries beyond agreed deadlines and amounts.	**Impacted** DLT is conceived of as being a write-only ledger system – as such a reversal would have to be dealt with through an opposing transaction on the ledger (which would be recorded as a new transaction).			
8	**Publication of Event Processing Rules** Event processing rules and templates should be harmonized as far as possible, and published in a coordinated way for global consumption and adherence.	**Not impacted** This principle refers to geographical harmonization of process, which ideally should carry through to DLT implementations as well.			Processing & reporting of corporate actions could be coded, enforced and controlled by through smart contracts or DLT chain logic.
9	**Protecting Investors' Rights** Clear rules concerning buyer protection, market claims (and any other instances where buyers' rights may be affected) should be established in each market and consistently followed, if possible by a central market infrastructure. Equally, consistent transformation methods should be established and applied.	**Impacted** This principle is impacted not by the nature of participation in the ledger but instead by the settlement cycle of the ledger. One aspect of DLT that is often highlighted is the possibility for T+instant settlement. If the ledger were to operate in this manner, buyer protection rules – which are designed to give rights to the buyer in the period between a trade and a settlement – would be unnecessary. If the DLT system were operating on a settlement schedule greater than T+instant, this principle would still apply.			Same as 8

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
10	**Electronic Voting** Issuers (or their agents) should take all necessary action to enable their shareholders to vote electronically. The definition of electronic voting must not be limited to the ability of shareholders (or their agents) to key votes manually into the issuers' (or their agents') web platform. The focus for electronic voting should be adherence to ISO format structured and standardized data where 'wholesale' voting is involved.	**Not impacted** We note however that this principle is not currently fully implemented today, and it still remains very much an issuer choice as to how voting is conducted at AGMs/EGMs (for instance, if this requires physical attendance at the meeting)			Same as 8
11	**Confirmation of Pre-meeting Vote Lodgment** Issuers (or their agents) should confirm the receipt of votes and, if found valid, that they will be cast in the general meeting as directed. If rejected, reasons why and (where possible) instructions and sufficient time to enable remediation should be given. Intermediaries should relay all communication immediately to the ultimate shareholders through the chain of investment. As with other corporate actions processing, electronic communication as outlined in Principle 1 should be the norm.	**No impact**	**Impacted** Intermediation chains are likely to be significantly reduced or removed in this model, thus making the transmission of information between issuer and investor a more direct process.	**Impacted** Intermediation chains are likely to be significantly reduced or removed in this model, thus making the transmission of information between issuer and investor a more direct process.	Same as 8
12	**Post-meeting Vote Confirmation** Issuers (or their agents) should confirm as soon as possible the execution of votes as instructed. Intermediaries in the chain should, in turn, confirm to all parties who participated in the voting, that their votes were cast, using the same communication channels as those through which the vote was received.	**No impact**	**Impacted** The considerations associated with principle 11 apply here.	**Impacted** The considerations associated with principle 11 apply here.	Same as 8
13	**Meeting Results** Upon receipt from the issuers (or their agents), market intermediaries should communicate the outcome of each voting event either directly or by notifying shareholders of the availability of the results on a public website.	**Not impacted**	**Impacted** The considerations associated with principle 11 apply here.	**Impacted** The considerations associated with principle 11 apply here.	Same as 8

6.8 Investment Funds

Principle		Model 1	Model 2	Model 3
1	**Paperless processes, straight-through processing based on ISO standards** Paper should be removed from all processing steps and replaced by STP processes. All trans-action related communication from order processing through commission payment between professional market participants should be electronic and adhere to ISO standards.	ISO 20022 standard is more than a messaging standard. It is a business modeling standards and as the fund industry have claimed over the years that ISO 20022 was the standard they want to use going forward, it is important that the business modeling standard is re-used in a DLT environment. The ISO 20022 standard has a data dictionary that describes the business elements that are needed in a fund transaction. It is important that those business elements are re-used in their ISO 20022 definition as it will allow interoperability, not only between DLT environments, but also with legacy messaging solutions.		
2	**Mitigation of operational risk** Financial and operational risks should be mitigated, especially counterparty credit risk and those related to the payment process.	**No impact**	The DLT environment could combine the cash process leg of the transaction, hence eliminating the credit risk and payment process issues.	
3	**Clarity of account structures** Distributors should agree with the fund management company prior to the first transaction how they will place orders, detailing the accounts in which their investments will be held and the accounts used for settlement. This should include details of any external third parties such as custodians or depositaries with whom the distributor has contracted for such services. The fund management company should in turn provide these details to their transfer agent.	Account could be obsolete in a DLT environment as only the transaction matters.		
4	**Key identifiers** Contractual agreements between a distributor and a fund management company should have a unique 'Agreement Identifier' and (where needed) a 'Local Identifier' which dictates the commercial terms to be applied in respect of all commission types. These identifiers should be quoted in all instructions relating to those agreements. The combined 'Agreement and Local Identifiers' and the relevant account numbers should be included in all fund orders.	**No impact**	**No impact**	**No impact**
5	**Commission reporting** Where omnibus accounts are used, order marking or equivalent standardized position reporting mechanisms should be in place to ensure correct commission calculation. A standard format for position reporting should be developed.	**No impact**	**No impact**	**No impact**

Principle		Model 1	Model 2	Model 3
6	**Fund Processing Passport** Fund management companies should provide a complete Fund Processing Passport (FPP) for all funds. The fund prospectus must mention where the passport can be obtained. The industry should get organized to facilitate access to and distribution of FPPs.	**No impact**	**No impact**	**No impact**
7	**Completeness of data throughout the intermediary chain** The order issuer is responsible for completing the order with all information required by the transfer agent. Each intermediary must pass on complete information.	**No impact**, except that some intermediaries might not be needed any longer.	**No impact**, except that some intermediaries might not be needed any longer.	**No impact**, except that some intermediaries might not be needed any longer.
8	**Acknowledgement of order receipt and confirmation of order execution** Transfer agents should acknowledge the receipt of orders as soon as possible. They should also notify the execution of orders as soon as possible. Distributors and client side custodians should send execution confirmations to their clients only upon receipt of an execution confirmation from the transfer agent.	**No impact**	**No impact**	**No impact**
9	**Flexibility of position reporting systems** Position tracking and reporting systems used by client side and fund side intermediaries as well as central market infrastructures, should support both trade date based and settlement date based reporting.	**No impact**	**No impact**	**No impact**
10	**Transfers of holdings** Transfers of holdings should be automated and, where possible, the distributor identifiers (combined Agreement and Local Identifier) should be included in the transfer instruction message.	**No impact**	**No impact**	**No impact**

6.9 OTC Derivatives

As part of gathering information and facts, the WG maintained a dialogue with various associations. It became clear that launching an ISSA initiative would duplicate industry-led efforts. ISSA therefore concluded that it would not seek to define operational solutions and/or standards as these are being worked on by associations like ISDA, SIFMA, ISITC and Managed Funds Association, to name a few. Information below is thus not sourced directly from ISSA documentation, however, relies heavily in particular on ISDA.

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
1	**Trade Capture** Once a transaction has been executed, both of the parties to the trade must enter the full terms of the transaction into their respective trade capture systems. The Trade Capture System, either independently or through a technological interface, should provide robust, accurate, reliable, real-time information related to credit risk, market risk and position exposure management, as well as provide trade support functionality to enable processes such as position verification, broker recaps, counterparty affirmations, confirmations, settlements, collateral margining, and financial control.	**Impacted** The interledger protocol of Model 1 will be a critical feature for trade capture as there are a number of touchpoints including collateral (cash/non-cash), financial control, settlement and position verification. These all need to operate in 'concert' to facilitate Trade capture. The standards however for each of these protocols	**Impacted** Trade capture is simplified in this model as information on positions and settlement is maintained directly by a counterpart and can be easily obtained with less reliance on third-parties such as CSDs and custodians.	**Impacted** As per model 2	Smart contracts can be used to automatically provide and capture information required for the trade

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
2	**Trade Capture Revisions** Trade capture revisions can be categorized as either economic or non-economic. Economic trade capture revisions can arise from any post-trade capture control processes, including during the risk management and position verification processes, or the broker recaps, counterparty affirmation and confirmation or settlements processes.	**Impacted** Items from point 1 will apply here, however it is important to note that trade capture revisions could be substantially limited in a DLT environment (across models) as much of the 'sequential' downstream processing is taken care of by the network particularly for events where smart contracts are used, much of these can be automated and with the immutable nature of the DLT appropriate controls can be applied in smart contracts which link the details of the trade to the various downstream processes. DLT is conceived of as being a write-only ledger system – as such a reversal would have to be dealt with through an opposing transaction on the ledger (which would be recorded as a new transaction).			
	Non-economic trade capture revisions can also arise from post-trade capture. Examples include an incorrectly identified broker, or a re-modeling of a transaction for internal purposes, where such re-modeling maintains the original economic intent of the transaction without altering the terms of the trade as agreed between the two parties. With the exception of electronic broker matching, Non-economic trade capture revisions will typically have minimal impact on downstream processing.	N/A negligent impact			
3	**Broker Re-cap** For trades executed via a broker, the broker recap process typically occurs on T or T+1 for standardized vanilla trade types (but may take place on a longer time frame for the more structured trade types). Traditionally, the broker will send a written recap of the economic details of the trade to both parties involved in the transaction by either facsimile or email. However, there is now some take-up of both the ability of parties to download their own broker recaps from a web portal, and also, increasingly, the available use of electronic broker matching. This independent third-party verification of trade details is used by each of the two contracting parties to validate the accuracy of their trade capture in order to gain confidence that the economic details of the trade are correctly understood and reflected in the official records of the parties concerned. This process often serves as the earliest point of risk mitigation in correctly securing the economic details of the trade.	**Impacted – Model 3 in particular** Model 3 would have a significant impact on this as broker matching and third party verification would be taken care of by the DLT.			

<table>
<tr><th colspan="2">Principle</th><th>Model 1</th><th>Model 2</th><th>Model 3</th><th>Potential for Smart Contracts</th></tr>
<tr><td>4</td><td><b>Counterparty Affirmation</b>
Counterparty affirmation also typically occurs on T or T+1. According to a party’s internal organization and processes, the counterparty affirmation process may be done (i) only for transactions that are traded direct (i.e. non-brokered transactions) and which are not confirmed with the counterparty by means of electronic matching, or (ii) for non-brokered transactions irrespective of the method used for the counterparty confirmation, or (iii) brokered and non-brokered trades which are not confirmed with the Counterparty by means of electronic matching, or (iv) all trades. The process is performed between the two parties to the transaction via telephone or through the delivery of a trade summary by email. It should be noted that some parties choose not to participate in the verbal affirmation process because their internal structural organization of resources’ responsibilities does not support this lifecycle event.</td><td colspan="3"><b>Impacted – model 3 in particular</b>
Counterparty affirmation of a trade could take place as part of the ‘single’ trade and settlement process. Accurate and corresponding trade summaries would be provided reciprocally to counterparts without the need to confirm these as the trade would already be effected.</td><td></td></tr>
<tr><td>5</td><td><b>Confirmation</b>
Confirmation is the process by which, either through electronic messaging or through the use of paper confirmations, the parties legally memorialize the terms of the trade. Confirmation is typically performed on T, or as soon as practical thereafter. Confirmation execution is the process by which the two parties confirm their agreement to the full terms of the trade as set out in the confirmation.</td><td><b>Impacted</b>
Interledger processes would facilitate standard electronic confirmations or using another ledger of the DLT to interact with.</td><td><b>Not impacted other than those in Model 1</b></td><td><b>Impacted</b>
Confirmations will be ‘read’ directly off the DLT. No need for separate processes on this point.</td><td></td></tr>
</table>

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
6	**Settlement** **(a) Pre-Settlement Activity** Settlement prices for transactions can be obtained either electronically or manually, but in any event should be done on a timely basis, at the latest the opening of business on the day following the day, or last day, of pricing in question. When obtained electronically, the relevant prices are taken from the price source through a technological interface, most commonly by way of a Logical Information Machine (LIM) feed or a data scrape of a particular website. When obtained manually, operations personnel will consult the appropriate price source based on the relevant pricing convention for the particular trade type and commodity product to be settled and manually input the relevant price(s). Best practices dictate that settlement prices that are input by one person (Maker) should be verified by a separate person (Checker).	**Impacted** Interledger protocols again will play an important role. Given the immutable nature of the DLT , it will be important to have smart contracts validating prices from LIM. Manual price upload would need to undergo a similar validation.	**Impacted** Same as Model 1	**Impacted** Same as Model 1	
7	**(b) Post-Settlement Activity** Once cash movements are effected, operations personnel will conduct a nostro reconciliation of ledger entries against cash movement. Discrepancies between cash and ledger entries are typically the result of failure to pay, underpayment or overpayment of agreed amounts, inadvertent payment to a different legal entity, or withholding of wire transfer fees. Operations personnel will investigate the discrepancies and resolve the matter via their individual organization's escalation controls, procedures and processes, but always with the goal of obtaining complete and accurate recording of cash movements (or exceptions) to the general ledger. Standard election option identification conventions should be adopted to facilitate the election process. Clear rules should be published by markets on the processing of reversals, which should be pre-advised in all cases and should require the prior consent of intermediaries beyond agreed deadlines and amounts.	**Impacted** DLT naturally resolves the reconciliation problem. Whether through interledger protocol or whereby all asset classes are on linked/same ledgers.			A 'DvP' concept could be applied here whereby cash receipt can be linked to a ledger entry.

Principle		Model 1	Model 2	Model 3	Potential for Smart Contracts
8	**Options** **(a) Financially Settled Options** Financially settled options are options that can be exercised automatically if, by comparing the reference price to the option strike price, the option is determined to be in-the-money. The option buyer is not required to give notice of exercise to the option seller. The automatic exercise will result in a payment by the option seller to the option buyer of the cash settlement amount, which may be netted with other transactions of the same commodity type and/or on the same settlement date.	**Negligible Impact**	**Negligible Impact**	**Impacted** See Smart contract application on a ledger which combines trade and settlement layers into one. This will provide considerable improvements in processing.	Smart contracts can facilitate the rules applied to options on a trade level and automatically execute settlement given predefined conditions. Particularly to model 3
9	**Close-Outs / Terminations** At any time during the term of a transaction, the parties may agree to terminate the transaction (i.e, end the trade early before its natural maturity date). The parties must agree on the terms, timing, and any payment relating to such termination. A termination agreement will be drafted and executed between the parties to memorialize this agreement.	**Only model 3 is impacted directly** This directly affects the trade conditions and if linked to smart contracts can be very effectively applied in DLT.			Same as 8
10	**Assignments and Novations** At any time during the term of a transaction, the parties may agree that one or both parties may transfer (by means of an assignment or a novation, as appropriate) their position to another party, which may be either an affiliate or an external party. All parties to the transfer must agree to the terms and timing of the transfer by executing either an assignment agreement or novation agreement, as applicable.	**Only model 3 is impacted directly (model 1 &2 are more focused around the settlement/custody aspects)** Peer to peer movement of holdings on the trade layer can be triggered by smart contract or a manual trigger which effects a smart contract.			Same as 8

6.10 High Level Potential Impacts on ISSA’s Inherent Risks Within the Global Custody Chain

In 2017 ISSA updated its original “Report on Global Custody Risks” document, reflecting the significant changes that have taken place in services for the custody of securities since its original publication in 1992. The new report, entitled Inherent Risks within the Global Custody Chain, outlines the various actors, processes and risks within the current global custody chain; rather than providing best practices it is an educational reference document.

With no DLT systems being currently used in a production environment, this working group has concluded that the time is not yet ripe to assess the impact of DLT on the content outlined in the Inherent Risks document in detail. The high level impacts below should be read with the understanding that this assessment was made from a perspective of DLT in theory, rather than DLT in practice.

Below, a short summary of the above-mentioned report is provided, followed by some none-exhaustive examples of potential impacts of DLT.

6.10.1 Brief Overview of the Content of Inherent Risks

Section 1 of the Inherent Risks document outlines the general principles of custody, pointing to intermediation in:

- The safekeeping of client / investor assets
- The settlement of securities
- The servicing of client assets
- Banking services
- Other services such as collateral management, securities financing and so on.

Based on intermediation in these areas, the document highlights the need for:

- Due diligence activity
- Reconciliation
- Adequate technology interfaces

Section 2 of Inherent Risks outlines the participants in the current custody lifecycle. Again, the level of intermediation in a DLT may have a significant impact on the nature of the roles outlined.

Section 3 examines the topic of asset and investor protection, providing detail in particular on:

- Account structures (distinguishing in particular between omnibus and segregated account structures)
- Investor protection regulation (highlighting a split between proprietary and client assets and considerations around regional differences in regulation regarding ownership of assets)
- Risk and the handling of insolvency or default events

Section 4 discusses client on-boarding procedures, with an emphasis on understanding the suitability and appropriateness of service providers throughout the custody chain.

Section 5 covers operational risks in various aspects of securities services, including services such as:

- Securities safekeeping
- Trade capture, clearing and settlement
- Asset servicing
- Foreign exchange
- Tax processing

Section 6 focuses on credit risk and mitigants thereof, highlighting:

- Delivery Versus Payment / Receipt Versus Payment settlement
- Standardised settlement cycles (in particular trade date plus 2 (or T+2) settlement)
- Contractual credit mitigants for custodians such as Lien or Pledge clauses
- Centralised clearing facilities provided by CCPs

Section 7 provides an overview of liquidity risk, again focusing on shortened settlement cycles, and highlighting the role of collateral management as a way of supporting liquidity.

Sections 8 and 9 examine information security and information technology risk.

Section 10 covers the management of vendor and outsourcing risk, focusing in particular on the network management function that has become crucial as custodial services have become more globalised

Section 11 focuses on the reputational, business and financial risks associated with (a lack of) adherence to regulation and compliance practices.

6.10.2 Examples of Potential Impacts

One finding to be drawn from the thematic impacts and other considerations is that DLT systems can be highly customized to fit into a wide variety of situations and use cases. Broadly speaking, differences in potential implementations highlighted in the above section can be summarized in the following table. When assessing the impact of a DLT implementation on the processes outlined in Inherent Risks, this may serve as a useful basis for analysis.

Unintermediated Participation (Issuer to end Investor)	Intermediated Participation in Network
Permissionless DLT	Permissioned DLT
General functional scope	Niche functional scope
Multi geographical/jurisdictional scope	Single geographical/jurisdictional scope
Multiple time zones	Single time zone
T+0 / T+Instant settlement	T+X settlement
Trading, clearing and settlement become the same process	Distinctions are maintained between trading, clearing and settlement
The DLT supports in-built business logic allowing for the automation of certain actions	The DLT has no internal business logic and solely records movements of transactions
“Digital native” assets	Tokenised representations of off-chain assets
Personal data stored on DLT	No personal data on DLT

Selected examples are provided below, outlining how some of the above elements may have impact on the content of Inherent Risks, were a DLT implementation to take place in a production environment. The analysis below remains largely theoretical at the present juncture and should be updated once concrete use cases become apparent.

6.10.3 Intermediation

Clearly, the level of intermediation in a DLT implementation would have an impact on a large number of the areas outlined above. For example, in an unintermediated environment where issuer and end investor are participants of the DLT, the needs for reconciliation highlighted in section 1 of Inherent risks would be substantially reduced, and the nature of due diligence activity would also substantially change to essentially being an activity the issuer conducts on the end investor and vice versa. The roles of intermediaries highlighted in section 2 would also likely change or disappear, as would concerns around proprietary versus client assets outlined in section 3. The custodian credit risk mitigants (i.e. Lien or Pledge clauses) highlighted in section 6 may rather apply to the provider of the DLT network, or indeed may not apply at all in a completely permissionless system without any form of centralised or governing party. Moreover the considerations around vendor and outsourcing risk highlighted in section 10 of Inherent Risks may be reduced through lower levels of intermediation.
It should be noted, however, that there is a spectrum of DLT implementations where levels of intermediation are maintained (i.e. the DLT is limited to a subset of custodian participants), where it is likely that the considerations outlined in the *Inherent Principles* would be unaffected.

6.10.4 Instant Settlement

The counterparty credit risks highlighted in section 6 could potentially be further reduced should the DLT allow settlement to take place at the same time as the trade (T+instant settlement), if the assets are blockchain-native. If the assets are not blockchain-native (i.e. if they are tokens of assets held elsewhere) the counterparty risk remains and would need to be mitigated by other means as one would have to assume that the tokenised assets correlate to the actual assets outside of the blockchain.

T+instant settlement would also potentially have implications for liquidity risk described in Section 7 of Inherent Risks. This is because T+instant settlement by its nature implies that settlement is conducted on a gross basis, without netting. This might lead to higher liquidity requirements as peaks would need to be covered.

It should be noted again, however, that T+instant is a design choice of the DLT system, rather than an obligatory characteristic of DLT implementations.

6.10.5 Process and Geographical Coverage

The functional scope and geographical reach of a DLT solution will be elements that may have a significant impact on the processes described in Inherent Risks. On the one hand, we could envisage a general functional scope that covers all processes related to securities services from issuance, through trading to custody. In this case, some of the operational risks outlined in section 5 of Inherent Risks would no longer be applicable – for example those related to the potential risk of failing to capture trade details accurately when performing settlement. Similarly, if we envisage a multijurisdictional DLT covering multiple markets, this may reduce some of the operational risks around securities safekeeping related to the selection of sub-custody structures outlined in section 5.

On the other hand, it is also possible that a DLT may have a very niche functional scope limited to one particular aspect of securities services. Aside from use cases aimed at providing DVP settlement on a DLT[7],[8], some niche DLTs are also currently in discussion. Examples include DLTs that focus on delivering systems to provide services for corporate

[7] http://deutsche-boerse.com/dbg-en/media-relations/press-releases/Joint-Deutsche-Bundesbank-and-Deutsche-Boerse-blockchain-prototype/2819826

[8] https://www.ubs.com/magazines/news-for-banks/en/products-and-services/2016/building-the-trust-engine.html

actions and proxy voting[9], while others target services related to cross border asset mobilisation for collateral management[10], repo transactions[11],[12].We also can observe DLT projects with national scope.[13] Niche DLT implementations may have impact on the description of such processes within Inherent Risks, but are unlikely to have a structural impact on the overall lifecycle of securities services it lays out.

6.11 Standards and Reference Data

While primarily descriptive in character, ISSA's report on Communication standards and reference data provides several recommendations with regard to immediate future challenges on the standardization of communications methodology. These are outlined below again with brief discussions of the potential impact of DLT.

6.11.1 Implement Trade Repositories with Standard Identifiers

The underlying goal of this recommendation is to encourage greater transparency and comparability of trades reported to different trade repositories. This recommendation still stands in a DLT context, however, the implementation may alter depending on the nature of the DLT network. It may be possible, for example, to harness in-built DLT business logic systems such as chain code or smart contracts to conduct this exercise. Alternatively TRs or regulators participating in a DLT network and extracting information with regard to transaction movements from it directly could be envsiaged, rather than putting a reporting obligation on individual participants.

6.11.2 Adopt and Build on the Legal Entity Identifier Standard

The adoption of LEI, as a standardized form of information, is likely not impacted by DLT, which would serve more as a means of transmission or distribution of information.

6.11.3 Drive for Increased Efficiency in Trade Confirmations and Allocations for Bonds, to Improve STP Rates

Here, the working group focused on the need for rapid confirmations or affirmations of trades between counterparties. In a DLT network where parties have access to the transactional information stored in the system, the need for such confirmations would be obviated between participants. Depending on the reach of the DLT network and the functional scope of the network this would have a greater or lesser impact on this recommendation. To take the example of the models:

Model 1 would likely lead to no impact on this recommendation, being a DLT distributed between a small number of intermediaries and there still being a functional difference between the trading and the settlement layer.

Model 2 would again likely lead to no impact on this recommendation, as although wider participation in the DLT network would be envisaged, the ledger would still be tracking movements of settled positions as opposed to trading.

Model 3 could lead to impact, as the trading and settlement processes could become the same. In this context, a trade affirmation or confirmation would be no longer necessary, as participants would be able to extract this data from the network itself.

[9] https://www.nsd.ru/en/press/ndcnews/index.php?id36=633471

[10] http://www.clearstream.com/clearstream-en/newsroom/170118/86346

[11] http://www.dtcc.com/news/2017/february/27/dtcc-and-digital-asset-move-to-next-phase

[12] http://otp.investis.com/clients/us/broadridge/usn/usnews-story.aspx?cid=928&newsid=48983

[13] http://www.asx.com.au/services/chess-replacement.htm

6.11.4 Facilitate the Coexistence of Post Trade Standards and Build on Interoperability between these Standards

As with recommendation 2, this recommendation is likely not impacted by DLT. What is more, this recommendation becomes more important, as DLT implementations must allow interoperability both with other DLT solutions and non-DLT systems so as not to lead to further fragmentation. This is why it is important to keep using the existing standards for reference data elements (e.g.ISO 6166 – ISIN, ISO 9362 – BIC, ISO 17442 – LEI, ISO 13616 – IBAN) and even the ISO 20022 data dictionary for the various business elements that will not change whether we are in a DLT environment or a legacy messaging to share information.

6.11.5 Encourage CCP Interoperability to Enable Firms to Concentrate their Clearing with One (or Two) CCPs to Achieve Margin and Operating Efficiencies

Again, as with recommendation 2, this recommendation is likely not impacted by DLT, outside of potential changes to the nature and role of CCPs in the lifecycle of securities services, as outlined elsewhere in the document.

Appendix 2

Regulatory Initiatives

1 Introduction

This appendix lists regulatory initiatives in the DLT space, specifically those that focus on the post-trade segment. The summary of ongoing initiatives is by no means intended to be exhaustive, either in terms geographical coverage, or in terms of covering all relevant developments. The area of FinTech is a fast-moving environment, and keeping on top of all relevant initiatives is and will continue to be a challenge.

Given that the intended focus of this report is on the post-trade segment of the securities industry, regulatory developments in the area of virtual currency (and in the payments space more generally) will not be looked at in this paper, though we will touch briefly on recent developments in connection with initial coin offerings ("ICOs"), which could produce some "overlap" for the securities space more generally.

As we will see, with a handful of exceptions, those regulators or legislators that have been looking at FinTech and innovation more generally appear to be taking a "wait and see" approach, preferring to promote innovation and experimentation and to regulate and legislate for activities actually undertaken, rather than seeking to regulate the technology itself.

2 Developing Trends

Whereas regulatory developments relating to innovation had arguably shown a tendency in the past to be fairly ad-hoc in their nature, a degree of coordination between regulators (consciously or otherwise) does appear to be developing.

By way of example, the series of ICO-related pronouncements (see par. 6 below) demonstrate that regulators are able to react swiftly in raising warning flags to market participants and investors, where they view it as necessary for investor protection reasons.

We have also seen a trend whereby regulators enter into cooperation agreements with one or more counterparts in other jurisdictions. Presumably it is only a matter of time before FinTech regulation generally, and specifically in the post-trade securities space becomes truly global in its nature.

3 Legal Considerations and FMI Principles

In addition to regulatory developments, there are undoubtedly a series of legal considerations that will arise as the adoption of DLT solutions picks up momentum. In the securities space, these include settlement finality, insolvency, and other matters of legal certainty. These issues are not addressed in this paper, so as to avoid introducing subjective interpretations of such issues.

For the time being, it seems clear that the use that is made of DLT technology in the securities space will have to be carried out within the spirit of the OICV-IOSCO principles that apply to financial market infrastructures[14].

[14] https://www.bis.org/cpmi/publ/d101a.pdf

4 Regulators and DLT

The regulators' role is a key consideration in terms of the governance of any DLT system.

The technology itself has the potential to bring key benefits for regulators. They could be granted access to view what is happening on the DLT network amongst entities and transactions they have supervisory authority over, albeit that they would have no greater permissioned access to information than is already the case under existing regulation.

The use of DLT could also have the effect of driving down costs and increase efficiency for the market as a whole. To the extent that DLT does not increase risks for participants and the market more generally, there should be no need for regulators to seek to regulate DLT itself.

The examples that have been drawn together in the remainder of this appendix serve to highlight that, for the time being, regulators appear to be taking care not to stifle innovation, whilst keeping a close eye on risks in the field of investor protection, for example.

5 ISSA Members' Interaction with Regulators

Judging by the regulators' stance to date, it is key for participants exploring the potential of DLT solutions for their business lines to engage early in the process with the regulators concerned. The regulators themselves are on a journey, and for the securities space in particular, it is key to "set the scene", distinguishing the DLT technology generally from the Bitcoin cryptocurrency (which ties in with the important distinction between "permissioned" and "permissionless" networks).

Regulators appear to have recognized the potential of DLT to reduce risk and to reduce the cost of capital formation. It is encouraging to see that certain regulators appear keen to work with each other on a bilateral or multilateral basis, and to share best practices. This is a positive development for firms that operate across several jurisdictions, and there does appear to be some early signs of commonality between regulators' approaches.

When engaging with regulators, however, firms should be aware that they may have to speak to more than one "branch" within a given regulator's operations – many regulators have established dedicated "innovation" departments, some of which sit within existing structures, whilst others are separate from, and in addition to, the more "traditional" branches of a regulator's organization.

6 Initial Coin Offerings

Initial Coin Offerings (ICOs) are receiving a lot of attention. ICOs are often mentioned in the same breath as Bitcoin and other well-known cryptocurrencies. Whilst the focus for the ISSA DLT group is the impact of DLT on the securities markets, it has been noted (by the SEC[15], ESMA[16], and other supervisory authorities internationally) that ICOs could, in certain circumstances, be caught by existing securities laws' requirements. The effect of which is that requirements around e.g. registration requirements and disclosure to investors must be followed. Various regulators have signaled their intention to increase their oversight of ICOs and other "token" like instruments.

[15] https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11

[16] https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf

Notwithstanding the general characterization that regulators have adopted a “wait and see” approach, the recent flurry of regulatory activity relating to ICOs has shown that, where one regulator makes a move (as the United States’ Securities and Exchange Commission did[17]), others have demonstrated that they are willing to follow suit and quickly (China[18], Hong Kong[19], Canada[20] and the United Kingdom[21]).

The developments in the field of ICOs serve to demonstrate the fast-moving nature of FinTech (including DLT), and how important it will be to stay on top of developments on the legislative and regulatory front. This will be just as crucial as keeping pace with the technology. Firms that overlook the potential regulatory considerations as part of the product development could come to find themselves undertaking regulated activities, and end up attracting attention for the wrong reasons.
In early February 2018, it was announced[22] that Gibraltar’s government was looking into a draft law to regulate the promotion, sale and distribution of ICOs connected with its territory. Separately, the French Autorité des marchés financiers (AMF) has recently consulted[23] on the definition of a specific legal framework for ICOs. Respondents to the consultation were said to have most strongly supported the option of proposing specific legislation adapted to ICOs. A key concern highlighted by the AMF was the need for information to be disclosed to investors.

The Austrian regulator has identified ICOs as one of its areas of focus[24], as has the German regulator, BaFin[25], which is said to be examining the issue on a case-by-case basis, rather than issuing new rule-sets governing ICOs. Likewise, the Japanese Financial Services Agency has issued a warning about the risks of ICOs[26]. In a press release dated 16 February 2018, the Swiss regulator, FINMA, announced the publication of updated guidelines in connection with ICOs (following on from guidelines that had been published in April 2017), and indicated that it saw (existing) money laundering and securities regulation as being most relevant to ICOs.

These examples aside, however, the emerging theme (as with the securities space more generally) seems very much to be that the regulators’ view is that, by and large, existing regulations are – for the time being at least – fit for purpose and can be applied to new asset classes. The use of a DLT solution to record interests in a given instrument does not change the substance of what, in effect, is still an offering of securities (with all the consequences that this entails).

[17] https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings
[18] http://www.miit.gov.cn/n1146290/n4388791/c5781140/content.html
[19] http://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=17PR117
[20] http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm
[21] https://www.fca.org.uk/news/statements/initial-coin-offerings
[22] https://uk.reuters.com/article/uk-gibraltar-markets-cryptocurrencies/gibraltar-moves-ahead-with-worlds-first-initial-coin-offering-rules-idUKKBN1FT1YX?utm_source=Exchange+Invest&utm_campaign=71f75e5d55-EI_daily_2016_12_13&utm_medium=email&utm_term=0_ea6bf736ef-71f75e5d55-417292709&mc_cid=71f75e5d55&mc_eid=9f12d27755
[23] http://www.amf-france.org/en_US/Actualites/Communiques-de-presse/AMF/annee-2018?docId=workspace%3A%2F%2FSpacesStore%2F57711a6c-4494-4215-993b-716870ffb182
[24] https://www.fma.gv.at/en/cross-sectoral-topics/fintech/fintech-navigator/
[25] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_180213_ICOs_Hinweisschreiben.html
[26] http://www.fsa.go.jp/policy/virtual_currency/07.pdf

7 International Coordination

7.1 G20

The G20, in its 2016 principles for digital financial inclusion spoke of the need to "provide an enabling and proportionate legal and regulatory framework for digital financial inclusion"[27]. Competent authorities around the world have begun the process of bringing forward new regulation in the domain of DLT, in the spirit of the G20 digital financial inclusion, for securities applications, though some countries' regulators have been more "pioneering" than others.

Whilst any substantive regulation has – to date at least – been initiated predominantly at jurisdictional level[28], there has been a degree of steer / alignment at the international level. At its 2016 meeting in China, the Group of Twenty ("G20") adopted eight high-level principles for "Digital Financial Inclusion"[29] (the "G20 High-Level Principles"). Principle 3, "Provide an Enabling and Proportionate Legal and Regulatory Framework for Digital Financial Inclusion", speaks of the need for:

> *"a legal and regulatory framework that is: predictable, risk-based and fair; allows for new entrants; and does not impose excessive, non-risk-based compliance costs".*

Without such an approach, the G20 continues, risks may not be adequately addressed, and the willingness to innovate and invest will be undermined.

7.2 OICV-IOSCO

In early 2017, OICV-IOSCO published a "Research Report on Financial Technologies (FinTech)"[30], which sets out the impact of FinTech on investors and financial services. The press release[31] accompanying the published report notes that "the global nature of FinTech therefore creates challenges that regulators should address through international cooperation and the exchange of information".

OICV-IOSCO noted in the report that, while regulation is typically overseen at a national or sub-national level, firms that make use of FinTech were likely to be operating at a global level. This "may create challenges in terms of regulatory consistency, as well as cross-border supervision and enforcement", and bring with it "a potential risk of regulatory arbitrage".

IOSCO noted that there has been multilateral collaboration at the level of IOSCO itself, as well as the CPMI[32], FSB and the BIS, as well as noting the importance of bilateral cooperation between national regulators. By way of example, IOSCO references

[27] Principle 3 of the G20 High-Level Principles for Digital Financial Inclusion, https://www.gpfi.org/sites/default/files/G20%20High%20Level%20Principles%20for%20Digital%20Financial%20Inclusion.pdf

[28] See. for example, a recent consultation and proposed legislative changes in France: https://www.tresor.economie.gouv.fr/Articles/tags/blockchain

[29] https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion

[30] http://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

[31] https://www.iosco.org/news/pdf/IOSCONEWS451.pdf

[32] See, for example, the CPMI's report on "Distributed ledger technology in payment, clearing and settlement https://www.bis.org/cpmi/publ/d157.htm

cooperation agreements that the FCA (UK) has entered into with other regulators, with a view to furthering the promotion of innovation in their respective markets[33].

7.3 Bank for International Settlements (BIS)

BIS published a report[34] in February 2017 which "provides an analytical framework for central banks and other authorities to review and analyse the use of distributed ledgers in payment, clearing and settlement activities". The report noted the following in relation to legal risk:

> *"Having a well-founded, clear, transparent, and enforceable legal basis is a core element of payment, clearing, and settlement arrangements. DLT can increase legal risks if there is ambiguity or lack of certainty about an arrangement's legal basis. Because the application of this technology to payment, clearing and settlement activity is new, the legal underpinning for certain activities may not be as well established as that for traditional systems (for example, in terms of identifying the applicable jurisdiction or relevant laws)."*

8 (European) Supranational Level

8.1 ESMA

At European Union level, a key regulatory body is the European Securities and Markets Authority ("ESMA"). ESMA set out its views on the application of DLT to securities markets in its report dated 7 February 2017[35], the main thrust of which was that it was premature to see what the regulatory response could or should be to the changes that DLT might be able to bring to the securities markets. In indicating that it would continue to monitor DLT-related market developments, ESMA took the view that active engagement by and between regulators was key to ensuring that DLT did not create unintended risks, and that its benefits were not hindered by "undue obstacles".

ESMA's approach here is perhaps best described as "wait and see", though a number of pieces of existing regulation were flagged as being likely to be of greatest relevance in the initial stages of considering the application of DLT to post-trade activities:

- European Market Infrastructure Regulation (EMIR) – certain classes of OTC derivative transactions have to be cleared through CCPs, an obligation that is extended by the Markets in Financial Instruments Regulation (MiFIR) to exchange-traded derivatives.
- Settlement Finality Directive (SFD) – intended to reduce systemic risk associated with participation in payment, clearing and securities settlement systems (and in particular the risks linked to insolvency of a participant in such a system)
- Central Securities Depositories Regulation (CSDR) – provides a set of common requirements for CSDs operating within the EU, harmonising certain aspects of the settlement cycle and settlement discipline.

[33] Example cited include agreements with the Republic of Korea's Financial Services Commission (https://www.fca.org.uk/publication/mou/fca-korean%20fsc-co-operation-agreement.pdf); the Monetary Authority of Singapore (https://www.fca.org.uk/publication/mou/fca-monetary-authority-of-singapore-co-operation-agreement.pdf); and the Australian Securities & Investments Commission (https://www.fca.org.uk/publication/mou/fca-asic-cooperation-agreement.pdf).

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

[35] https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

Distributed ledger technology has been included as one of the areas that ESMA will monitor in the course of 2018[36] by analyzing emerging and existing instruments, platforms and technology. It sees financial innovation as a "cross-cutting activity", and notes that advances in the DLT space, which "continue with high frequency" call for ongoing monitoring. ESMA's wait and see approach in the post trade space contrasts with that taken by the European Supervisory Authorities in relation to virtual currencies, where a pan-EU warning has been issued[37], and ESMA's statements concerning Initial Coin Offerings (ICOs)[38].

In its response[39] to the European Commission's consultation paper on FinTech, ESMA noted (in June 2017) that it would be premature to assess the changes that DLT could bring to the securities markets, and the regulatory response that might be required. Nor, however, did it identify any "major impediments in the existing EU regulatory framework that would prevent the emergence of DLT in the short term".

ESMA flagged in its February 2017 report[40] the expectation that DLT was "likely to be used primarily for post-trading activities", but considered that existing regulatory frameworks such as EMIR, SFD, CSDR, MIFID/MIFIR and the like did not require immediate adjustment as a consequence of DLT being deployed. ESMA has, however, noted that it is important for regulators at the EU and international level to engage and cooperate with each other, noting that some national authorities were looking to encourage innovation and that this could give rise to unintended consequences, including regulatory arbitrage.

8.2 European Central Bank (ECB)

In an occasional paper published in April 2016 by two authors at the ECB (which paper did not, however, represent the views of the ECB), the potential of blockchain was said to be that it could bring gradual change, to securities post-trading, rather than to be revolutionary. In line with the views expressed elsewhere, it was acknowledged that innovation was generally welcome, for as long as it could bring safety and efficiency. Just as existing regulatory frameworks are thought to be fit for purpose for the time being, it was mentioned that certain post-trade functions would continue to be performed by institutions.

8.3 European Commission

The European Commission published a public consultation on FinTech[41], the intention behind which was to gather "input from stakeholders to further develop the Commission's policy approach towards technological innovation in financial services". The areas covered in the questionnaire were as follows:

- Fostering access to financial services for consumers and businesses.
- Bringing down operational costs and increasing efficiency for the industry.
- Making the single market more competitive by lowering barriers to entry.

[36] See ESMA's Supervisory Convergence Work Programme for 2018 (https://www.esma.europa.eu/sites/default/files/library/esma42-114-540_2018_supervisory_convergence_work_programme.pdf)

[37] https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-risks-in-buying-virtual-currencies

[38] https://www.esma.europa.eu/sites/default/files/library/esma71-99-649_press_release_ico_statements.pdf

[39] https://www.esma.europa.eu/sites/default/files/library/esma50-158-457_response_to_the_ec_consultation_on_fintech.pdf

[40] https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

[41] https://ec.europa.eu/info/finance-consultations-2017-fintech_en

- Balancing greater data sharing and transparency with data security and protection needs.

Input was requested on a broad range of matters, including the potential application of DLT in securities markets. The Commission noted that ESMA had previously consulted on DLT applied to securities markets, and that it had concluded that regulatory action was premature. Nevertheless, it sought input from stakeholders on how the application of DLT could best be facilitated in the financial industry, whilst safeguarding market integrity, investor protection and financial stability.

In particular, the Commission noted one potential use case of DLT being in the area of post-trade, suggesting that DLT had the potential to disintermediate and automate processes and to reduce counterparty and operational risk. Other use cases included better access to voting in general shareholders' or bondholders' meetings, said to improve governance.

The Commission held its first FinTech & Digital Innovation Conference in February 2017. This followed on from the establishment in November 2016 of an internal Task Force on Financial Technology[42], the aim of which is "to assess and make the most of innovation in this area, while also developing strategies to address the potential challenges that FinTech poses".

Most recently, the European Commission announced[43] the launch of its FinTech Action Plan in February 2018, the three main goals of which are to:

- Support innovative business models to scale up across the single market.
- Encourage the uptake of new technologies in the financial sector.
- Increase cybersecurity and the integrity of the financial system.

The Commission also announced that it would invite the European Supervisory Authorities to identify best practices for innovation hubs and sandboxes. Although mention was made of cryptocurrencies, no specific mention was made of the (post-trade) securities markets.

Several European Union member states have taken steps to foster the development of FinTech – some developments are noted further below.

8.4 Recent Developments at European Union Level

The European Commission adopted its "FinTech Action plan"[44] in March 2018. The action plan forms part of the European Commission's efforts to build a capital markets union, and is linked to its aims relating to the digital single market.

It aims to foster initiatives to "enhance supervisory convergence toward technological innovation and prepare the EU financial sector to better embrace the opportunities brought by new technologies"[45].

Particular mention is made of "crypto-assets". Whilst, as noted elsewhere in this section and other parts of this paper, regulatory pronouncements to date have focussed on virtual currencies, ICOs and the like, the European Commission indicates in its action plan that it (in conjunction with other relevant regulators [e.g. the ESAs and the ECB]) will monitor this area closely in the course of 2018, with a view to assessing whether specific regulatory action at EU level is required.

[42] See press release here: http://europa.eu/rapid/press-release_MEX-16-3691_en.htm

[43] https://ec.europa.eu/commission/commissioners/2014-2019/dombrovskis/announcements/vp-dombrovskis-speech-afore-consultings-2nd-annual-fintech-and-digitalisation-conference_en

[44] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109

[45] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/fintech_en

Also of interest is the intention to establish an "EU FinTech Lab", the aim of which is apparently to bring multiple (EU) vendors together with regulators and supervisors, to create a forum in which regulatory and supervisory concerns can be discussed.

8.5 General Data Protection Regulation (GDPR)

The EU's GDPR came into effect on 25 May 2018. There are open questions as to exactly how existing or future applications of DLT generally should ensure that they are and remain compliant with GDPR. A key issue will be how the "immutability" of a DLT-based system can be upheld, whilst respecting the right of data subjects to require erasure of certain data, or to have data transmitted elsewhere (data portability).

There has been some fairly recent comment on this on a blog published on the R3 website[46], which makes clear that GDPR will be a challenge for the blockchain industry generally, albeit that those challenges may not be insurmountable (e.g. personal data which might be caught by the GDPR obligations could be held outside the DLT environment).

9 National Level

9.1 Australia

The Australian regulator, the Australian Securities & Investments Commission (ASIC) has established an innovation hub[47], which assists FinTech start-ups developing innovative financial products or services to navigate the regulatory system. Similar to the FCA's sandbox, ASIC has indicated that there are waivers and relief from regulatory and compliance requirements which might assist businesses in innovating.

A FinTech licensing exemption has been established, with two class waivers to allow eligible businesses to test specific services or products for up to 12 months with up to 100 retail clients without holding the relevant licence.

In an information sheet issued in March 2017[48], ASIC stated that it believed that the existing regulatory framework is able to accommodate the DLT use cases that it had seen, but that it anticipated that additional regulatory considerations might arise as DLT matures (ASIC is the regulator that is overseeing ASX).

9.2 Belgium

The Belgian government-backed innovation platform, B-Hive (formerly known as Eggsplore) recently sent a delegation to London in a bid to build a bridge between the FinTech communities of London and Brussels[49]. The stated aim of the platform is to provide value to all organisations that are dealing with the impact of digital technology on the financial system, by bringing together different actors and to (amongst others) explore opportunities offered by digital transformation, and jointly promote know-how. The Belgian government is not understood to have legislated in this domain yet, however (unlike their French counterparts).

9.3 Canada

The Canadian Securities Administrators have established a regulatory sandbox[50], which is aimed at allowing FinTech firms to register or obtain relief from securities law

[46] https://www.r3.com/blog/gdpr/

[47] http://asic.gov.au/for-business/your-business/innovation-hub/

[48] http://asic.gov.au/regulatory-resources/digital-transformation/evaluating-distributed-ledger-technology/

[49] https://b-hive.eu/events-1/2017/4/25/finandtonic-on-gdpr

[50] https://www.securities-administrators.ca/industry_resources.aspx?id=1588

requirements. Like the UK FCA's sandbox initiative, the CSA Regulatory Sandbox provides an environment in which firms can test their products on a time-limited basis.

Separately, Quebec's Autorité des marchés financiers (AMF) announced at the end of April 2017[51] that it had joined the R3 blockchain consortium and created a FinTech lab to advance its response to new technologies.

Most recently, the Canadian securities regulatory authorities from across Canada announced on 8 February 2018[52] that they had entered into a cooperation agreement with France's Autorité des marchés financiers (AMF), under which the regulators will share certain information, provide support to firms, share expertise and foster a dialogue on FinTech and innovation in finance more generally.

9.4 People's Republic of China

A paper published by staff members of the Chinese Banking Regulatory Commission (CBRC) (though the paper does not apparently represent the official position of the CBRC) was reported[53] to have suggested that, to respond to potential risks created by blockchain, the Chinese securities market would need new rules. The paper also suggested that the central government should take the lead in developing a blockchain industry standard, rather than allowing firms to develop such a standard.

The authors mentioned moves that had been made by other countries' regulators, recommending, for example, that the Chinese authorities create a regulatory sandbox to allow for controlled development and testing of products.

9.5 France

As part of the implementation of a legislative reform to bring greater transparency, fight corruption and to modernize the economy[54], the French Treasury has recently announced a public consultation[55] on the use of blockchain for certain financial securities. The aim is to allow interested parties to comment on the scope, principles and applicable regulatory framework for the development of a blockchain securities platform for securities not issued through a central securities depository or transferred through a securities settlement system. Amendments to existing securities legislation may be required, though, as noted in the section above dealing with European Union-level regulations, there may be limits as to the possibilities here.

9.6 Hong Kong

The Hong Kong Monetary Authority commissioned a White Paper[56], the aim of which was to look at the potential, risks and regulatory implications of DLT, and to identify possible applications of DLT to banking services through Proof of Concept work. In addition to potential domestic legal concerns relating to data privacy, litigation and compliance, the paper noted (as mentioned in the introduction to this present paper) that questions were being raised more internationally in connection with fundamental legal matters such as

[51] https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/amf-creates-fintech-lab-and-signs-partnership-with-r3/

[52] https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/canadian-securities-regulators-sign-agreement-with-the-french-autorite-des-marches-financiers/

[53] https://www.coindesk.com/chinas-banking-regulators-push-blockchain-securities-rules/

[54] The law was promulgated in December 2016, and is referred to as "Sapin II". More information is available here: http://www.senat.fr/espace_presse/actualites/201606/le_senat_examine_la_loi_sapin_2.html

[55] The consultation closed on 19 May 2017 http://www.tresor.economie.gouv.fr/16101_consultation-publique-ordonnance-blockchain-applicable-a-certains-titres-financiers

[56] http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf

applicable law, rights and obligations (and their enforcement), liability for systems and enforcement of a system's rules and procedures. It has been noted above that the UK's FCA had concluded a number of bilateral agreements with its counterpart in several other countries across the globe. The Hong Kong Monetary Authority (HKMA) was one such example. HKMA has been particularly active in the FinTech space, having established a "FinTech Facilitation Office"[57], whose stated aim is to "facilitate the healthy development of the FinTech ecosystem in Hong Kong and to promote Hong Kong as a FinTech hub in Asia".

In addition, the HKMA launched (in late 2016) a FinTech supervisory sandbox, which allows banks and FinTech firms to conduct (limited) pilot trials of their FinTech initiatives, without the need to be fully compliant with HKMA's supervisory requirements. The sandbox was overhauled in September 2017, with the establishment of a "chatroom", allowing tech firms to access the sandbox (and seek feedback) without having to pass through a bank. In addition, in a bid to facilitate trials of cross-sector financial products, the HKMA's sandbox was linked up with sandboxes operated by the Securities and Futures Commission (SFC) and the Insurance Authority (IA).

HKMA is also understood to have been looking into digital currency-related research, together with a number of banks and industry consortium R3[58].

9.7 Japan

The Bank of Japan and the ECB launched a joint research project in December 2016 (codenamed "Stella"), the intention behind which was too investigate the possible use of DLT for financial market infrastructures. In a September 2017 communication[59], the BOJ and ECB noted that, whilst the various solutions tested (the liquidity saving mechanisms of BOJ-NET and TARGET2 were among the cases tested) were found to be fairly resilient, no direct conclusions could be reached based on the tests alone. Indeed, the central banks went as far as concluding that, given its relative immaturity, DLT could not be said to be a solution for large scale applications such as their RTGS payment systems. In March 2018 the two central banks issued a joint report[60] for the second phase of the joint research project "Stella" which dealt with the exploration of DVP in a DLT environment (single ledger or cross-ledger).

Away from the payments sphere, the Japanese Financial Services Agency (JFSA) is thought to be interested in looking at how blockchain has the potential to transform the financial and economic landscapes, and announced in March 2017[61] an initiative to encourage multilateral joint research on financial trading on blockchains. Back in 2016, the JFSA indicated its intention to conduct forward-looking analysis on the potential impact of FinTech on the financial industry generally.

9.8 Luxembourg

Although it is understood to take the same technology-neutral approach as its counterparts in other jurisdictions, one of the government divisions has a mandate that specifically includes financial innovation, in addition to following international and national regulatory developments. [62]

[57] https://ffo.hkma.gov.hk/

[58] http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171024e1.pdf - Paragraph 3.4

[59] https://www.ecb.europa.eu/paym/intro/news/shared/20170906_stella_report_leaflet.pdf

[60] http://www.boj.or.jp/en/announcements/release_2018/data/rel180327a1.pdf

[61] http://www.fsa.go.jp/en/news/2017/20170309-2.html

[62] http://www.fsa.go.jp/en/news/2017/20170309-2.html

9.9 The Netherlands

The Authority for Financial Markets (AFM) and De Nederlandsche Bank (DNB) have jointly established the "InnovationHub"[63], which is intended to provide support to companies that are looking to bring innovative financial products to market, but which have doubts as to the applicable supervision and regulation. The regulators have also established a "regulatory sandbox"[64], the stated premise of which is to allow the AFM and DNB to focus on the "real purposes" of the ruleset when assessing innovative products, services or business models. Interestingly, it is open to new and established market players alike. The sandbox is intended to be used where specific (and, presumably, existing) policies, rules or regulations cannot reasonably be met by the company that is looking to provide an innovative product or service.

9.10 Poland

The Polish Ministry of Digital Affairs has adopted a new proposal designed to allow the local blockchain industry to self-regulate[65].

9.11 Russian Federation

The Bank of Russia has repeatedly issued statements favoring DLT as technology and discouraging cryptocurrencies. It has also been stated that the regulation and laws only govern the business applications utilizing DLT and not the technology explicitly and that as long as DLT solutions don't contradict existing laws, they may be employed as desired by the market participants.

On the subject of crypto assets, the Bank of Russia has stated support to the crypto assets overall, but insists on their regulated circulation being compliant with all current and upcoming laws. Effectively, cryptocurrencies like Bitcoin are discouraged from use and it is understood by the market that only compliant crypto assets will be accepted by the regulator when the laws and regulation are formalized.

There has been an active discussion in the Bank of Russia, Ministry of Finance, Russian Parliament and various startup and industry professionals on the regulation of crypto assets. As of April 2018, there are two law proposals registered in the Parliament, one dealing with the general definitions of the crypto assets, and the other defining and establishing rules of crowdfunding activities, including ICOs. Additionally, there is a proposal to update the Civil Code law to provide the same definitions and to allow cryptocurrencies to be used within the legal framework. It is expected that some combination of these laws will take effect in 2018, bringing certainty and compliance to the DLT use in Russia.

9.12 South Africa

In South Africa, the Intergovernmental FinTech Working Group (IFWG) was formed by members from National Treasury (NT), the South African Reserve Bank (SARB), Financial Services Board (FSB) and Financial Intelligence Centre (FIC) at the end of 2016. The objectives of the IFWG were to enable policymakers and regulators to understand, more broadly, the financial technology (FinTech) developments and relevant policy and regulatory implications for the South African financial sector and economy in order that a coordinated approach could be developed and adopted. The overall objective was to foster FinTech innovation while ensuring the continued efficient functioning of financial markets, financial stability and protecting the rights and interests of customers and investors.

[63] https://www.afm.nl/en/professionals/onderwerpen/innovation-hub
[64] https://www.afm.nl/en/professionals/onderwerpen/innovationhub-maatwerk
[65] http://www.coindesk.com/poland-digital-ministry-best-practices/

9.13 United Kingdom

The Financial Conduct Authority (FCA) has established a project called "Project Innovate"[66], to assist in the promotion of FinTech and innovative businesses. As part of the project, the FCA has established a "regulatory sandbox"[67] to allow authorised and unauthorised businesses alike to obtain clarity around applicable rules (for authorised firms), or for unauthorised firms to test their innovation in a live environment.

The Bank of England (BoE) has set up a FinTech Accelerator[68], as part of which the BoE is working in partnership with FinTech companies to look at the application of FinTech innovations for central banking. A proof of concept[69] (POC) was undertaken in partnership with PwC, based on a use case of transfer of ownership of a fictional asset among several participants, including a central authority. The POC demonstrated concepts seen in real world scenarios of gross settlement and transfer of value.

The FCA published a discussion paper[70] on 10 April 2017, the stated aim of which is to "to start a dialogue on the potential for future development of distributed ledger technology (DLT) in the markets we regulate". The FCA noted that it generally takes a 'technology neutral' approach to regulating financial services and [is] interested in considering whether there is anything distinctive about DLT which would require [it] to take a different approach". The FCA is currently reviewing responses and will then decide on next steps.

Adopted on 29 March 2017, the best practices cover areas related to the activities of cryptocurrency companies including their recommended legal form, transparency, legality of operations, relations with public authorities, customer relations, technology and security, as well as their stance toward customers and business partners.

9.14 United States of America

Any regulation that has emerged in the DLT space has come at state level, albeit that the Federal Reserve Board has previously spoken about the evolution of blockchain, calling it "the most significant development in many years" in how financial assets are traded[71].

At state level, states such as Nevada, Vermont and Arizona have passed blockchain-related legislation. Nevada authorities passed a law in June 2017[72] which adds a definition of blockchain, and specifies that "electronic records" include blockchain. In Vermont, the law provided a definition for blockchain, and recognized documents notarized on a blockchain as having probative value. Finally, Arizona has enacted a law that recognizes blockchain signatures and smart contracts.

[66] https://www.fca.org.uk/firms/fca-innovate

[67] https://www.fca.org.uk/firms/project-innovate-innovation-hub/regulatory-sandbox

[68] http://www.bankofengland.co.uk/Pages/fintech/default.aspx

[69] http://www.bankofengland.co.uk/Documents/fintech/fintechpocdlt.pdf

[70] https://www.fca.org.uk/publications/discussion-papers/dp17-3-discussion-paper-distributed-ledger-technology

[71] https://www.reuters.com/article/us-usa-fed-brainard/feds-brainard-sees-blockchain-as-revolutionary-but-still-to-prove-itself-idUSKCN1272BG?feedType=RSS&feedName=topNews

[72] https://www.nvbar.org/wp-content/uploads/NevadaLawyer_Aug2017_Blockchain-1.pdf

Appendix 3

Information Security Terms Explained

1 Consensus Protocols

Achieving consensus is complex, and models have to be able to deal with a range of potential failures including message delays, network partitions and forks, node failures and corrupted messages. These failures may be malicious in nature.

Different models approach this by using their own set of algorithms to address the potential types of failure. In general the properties that each algorithm looks to address cover Safety, Liveness and Fault Tolerance.

Safety is the ability to have all nodes generate the same output and that this output is valid according to the rules of the consensus protocol. Liveness refers to the ability for all nodes to generate an outcome or value.

Fault Tolerance covers the ability to recover from node failures and still achieve a consensus outcome. Fault Tolerance talks to two core types of failure in distributed ledger systems. Fail stop faults – where node failures cause nodes to stop participating in the consensus process, caused by software or hardware failures.

The second category is Byzantine faults where nodes can act erratically, either due to software bugs or nodes becoming compromised. The focus on Byzantine failures is to ensure that a small number or erratic nodes do not compromise the actions of the valid or good nodes in the network.

Tolerating Byzantine adds a significant level of complexity to the consensus protocol as it forces us to add additional messaging layers into the system or model. Practical Byzantine Fault Tolerance (PBFT) was the first model that achieved BFT with a relatively low overhead and uses a model of primary and secondary replicas to check and validate the decisions made by the primary replica.

2 Proof of Work (PoW)

PoW is an approach most frequently used in permissionless distributed ledgers today. It is used in both Bitcoin and Ethereum among others.

The PoW mechanism makes nodes, called “miners”, solve computationally intensive mathematical problems, like trying to brute-force non-invertible hash functions, in order to add blocks to the ledger. Computing power is a scarce resource and expensive to operate (it takes electricity and requires powerful servers). The protocol relies on the incentive of those expending significant computing power to observe the ledger rules, so that their version of the ledger does not get overturned by the majority and their expended computational power does not go to waste. With this incentive it requires the attacker seeking to bypass the consensus to own more than half of the ledgers total computational power, which is prohibitively expensive.

The significant drawback of the PoW protocol is the large amount of resources required to operate the ledger. These resources are required to protect the ledgers from malicious attacks, so they can’t be optimized.

The method also restricts throughput of the network. Since each transaction needs to be confirmed using expensive computation, the scalability of the network is limited by the total amount of computation that the ledger has in its disposal.

3 Proof of Stake (PoS)

PoS models replace the mining models used in Proof of Work with an alternative approach that involves the user's stake or ownership in the virtual currency of the platform being committed against the validity of consensus authentication.

The PoS algorithm randomly selects validators for block creation, where validators commit stakes to increase the likelihood of being selected as a validator. However, the algorithm ensures that the process is entirely random, so that no node can predict the work that it will be asked to perform. The nodes have an incentive to validate transactions properly, because if their version of the ledger is rejected, they will lose their stake.

Ethereum Casper and Serenity algorithms are examples of PoS models, where nodes are bonded to the system by their advance stakes that are committed to the system.

4 Proof of Elapsed Time (PoET)

The PoET model was developed originally by Intel to run in a Trusted Execution Environment (TEE) such as Intel's SGX (Software Guard Extensions). The model uses a lottery system to elect the next leader to finalise the block, based on the assessment of all available nodes, and uses the TEE to guarantee the safety and randomness of the process.

The PoET model works by validators requesting wait times from their TEE system, and the validator with the shortest wait time will win the lottery. Wait times are generated randomly and this protects the randomness of the protocol. This only material drawback on this model is the reliance on the TEE.

5 Practical Byzantine Fault Tolerance (PBFT) Derivatives

Hyperledger Fabric was developed by the Linux Foundation as a model that is developed purely for permissioned systems where all participants are verified and validated by the central registry for the system. Hyperledger supports two consensus models – PBFT and SIEVE – a variant of PBFT that supports non-deterministic chaincode execution.

Participants are identified as either a validating or a non-validating peer. The validating peer (VP) is a node in the system responsible for the consensus validation process and the maintenance of the ledger. Non-validating peers operate as a proxy to connect clients with validating peers, they are not capable of executing transactions but are able to verify them. The Fabric platform enables clients to manage transactions by using smart contracts or chain codes, endorsing peers and an ordering service. Chain code implements a prescribed interface and runs in a secured Docker Container separated from the endorsing peer process. The code is implemented in the Fabric network, where it is executed and then validated by the endorsing peers who manage the ledger, the database and follow the network policies. The ordering service holds the task of creating blocks for the ledger and manage in what order the blocks are added.

The PBFT is a mathematical algorithm based on transaction being broadcasted and then responses from all participants are collected and verified before deciding whether it is a valid transaction block or not. It works on the assumption that no more than 1/3 of participants are faulty The mechanism uses Validating Peers (VP), trusted nodes, and a leader of the network. When a transaction is requested, a VP validates the transaction and broadcasts it to the rest of the VPs. After a batch timeout (couple of seconds) the leader builds a block from the transaction and broadcasts the block to the VPs for consensus on the block by using the PBFT algorithm. If consensus is reached on its validity all the VPs execute the transaction and thereby add another block to the private blockchain. It provides important optimizations, ensuring encryption of messages while also reducing their size for the systems to be manageable to Byzantine faults. The PBFT aspects ensure there is no deadlock in the communication where two participants indefinitely wait for the other participant's response. PBFT imposes a low overhead on the replicated service performance.

SIEVE is an adjustment of PBFT that is non-deterministic and therefore produces different outputs when executed by different replicas. It processes all activities separately and then reviews the outputs to look for alignment in these. If it identifies a small deviation from a norm it removes the nodes through sieving these out; if it finds divergence across a number of core processes then these too will be sidelined.

6 Federated Consensus

Ripple and Stellar are variants on the BFT model that differ by making these open ended in terms of the participation of nodes, a feature that has made them specially applicable to payment system models.

All participants are end users in these model, financial institutions are termed gateways. Gateways are generally regular banks that hold currency accounts for clients, and create equivalent values in the blockchain to allow for real-time payment processing. Market makers provide liquidity to the network and may be both users of gateways.

Ripple and Stellar use a BFT variant consensus model that allows them to adapt to the roles that Uses, Gateways and Market Makers perform.

Ripple operates the Ripple Consensus Protocol Algorithm where each node creates a Unique Node List (UNL) that defines the trusted counterparts that it has contracted with. The consensus model operates by each node leveraging its UNL where each node collects its transactions into a data structure called a Candidate Set and communicates its candidate sets with other UNL nodes, where each votes on the transactions and these are then refined with the transactions achieving the highest votes moving to the next round. When a candidate set reaches 80% votes it becomes a valid Ripple block. The next candidate chain comprises new transactions and those that were not finalized in the previous block, and so forth.

Stellar Consensus Protocol leverages a concept of quorums and quorum slices to drive its consensus protocol. Quorum is the number of nodes required to reach agreement and the slice a subset of this. The model allows a node to select other nodes that can participate in reaching agreement on transactional validity, mirroring the business relationships that exist today and hence the trust mechanisms already present in bilateral business relationships.

Appendix 4

Working Group Members

Urs Sauer, SIX Securities & Exchanges (Working Group Lead)

Charles-Raymond Boniver, Swift (Work Stream Co-Lead)

Giles Elliott, Tata (Work Stream Lead)

Christopher Hollifield, Clearstream (Work Stream Co-Lead)

Stephen Lindsay, Swift (Work Stream Co-Lead)

Raymond Mallon, Euroclear, (Work Stream Lead)

Hariprasad Bantwal, Credit Suisse

Jérôme Boulanger, Clearstream

Alexander Chekanov, NSD Russia

Chris Church, Digital Asset Holdings

Brian Crabtree, Citibank

Warren Dunne, HSBC

Steve Everett, Strate

Mariangela Fumagalli, BNP Paribas Securities Services

David Guest, UBS AG

Georg Imboden, SIX Securities Services

Emma Johnson, Deutsche Bank

Graham Kellen, Schroders

Elizabeth Maiellano, Broadridge

Karla McKenna, Citibank

Dan O'Prey, Digital Asset Holdings

Robert Palatnick, DTCC

Jennifer Peve, DTCC

Angus Scott, Euroclear / CLS

Jack Sellers, HSBC

Derren Selvarajah, Standard Chartered Bank

Fabrice Tomenko, Clearstream

Fabian Vandenreydt, B-Hive

Maria R. Vermaas, Strate

Marc Wetjen, DTCC

Jill Whitney, Broadridge

Axelle Wurmser, BNP Paribas Securities Services