Whitepaper 2.0
on Distributed Ledger Technology

25 October 2017

HONG KONG MONETARY AUTHORITY
香港金融管理局

Whitepaper 2.0
on Distributed Ledger Technology

Table of Contents

Chapter 1

Foreword

Many people have commented that, if 2016 was a year of proofs-of-concept (PoCs) for distributed ledger technology (DLT), then 2017 should be a year of prototypes and production. Although the deployment of DLT projects into production on a large scale is still uncommon, small-scale pilot runs putting DLT on trial are regularly reported from different corners of the world. From what we have observed in the market, the technology per se is probably not the greatest hurdle to large-scale roll-out of DLT projects. More often, it is the governance, control and legal issues associated with the technology, and the new risks that come with it, that are proving the toughest challenges for the industry to deal with. Differences in legal regimes across different jurisdictions certainly do not help, and indeed are often exacerbating the situation.

Last year, the Fintech Facilitation Office (FFO) of the Hong Kong Monetary Authority commissioned the Hong Kong Applied Science and Technology Research Institute to conduct a research project on DLT. In the first stage of the project, a whitepaper was published to outline the key features, benefits, risks and potential of this technology. Following PoC work carried out by banks and other industry players on three banking services (trade finance, digital identity management and mortgage loan applications), the whitepaper also shared the experience gained from these projects.

This year the FFO has continued to engage with the participating banks and other industry players to complete the PoC projects, while at the same time carrying out research into the governance, control, compliance and legal issues related to DLT implementation. These issues are addressed in this second whitepaper. I would like to express my gratitude to the many industry experts and professionals who have contributed thematic articles on various topics around the implementation of DLT.

This second whitepaper is unique because it has devoted substantial parts to offering practical advice. Based on the real-world experience gained from the PoC projects and the specialist knowledge of professional practitioners, it provides pragmatic suggestions and guidance on implementing DLT, especially in terms of governance controls and legal considerations. Accordingly it will, we hope, help facilitate the sound and safe implementation of DLT for financial applications.

Another fruitful result of the PoC projects has been the plan to progress the trade finance PoC into the Hong Kong Trade Finance Platform, where digitalised trade documents will help automate the trade finance process to reduce risks and increase the financing capability of the banking industry. The platform will also try out a “connectivity highway” to address the issue of interoperability with similar DLT-based trade platforms in other jurisdictions.

It is vital for Hong Kong to explore the potential of DLT and deploy the technology where it offers significant benefits, so as to maintain the city’s status as an important global financial centre. When applying DLT to financial applications, risks have to be minimised and the interests of the general public protected. Now that the value of DLT has been demonstrated and the technology is out of its infancy, I trust that this whitepaper will serve as a timely reference document for the implementation of DLT in the banking and payment industries.

Howard Lee
Senior Executive Director
Hong Kong Monetary Authority

Chapter 2

Executive Summary

2.1 Introduction

In 2016, the Hong Kong Monetary Authority (HKMA) commissioned the Hong Kong Applied Science and Technology Research Institute (ASTRI) to conduct an in-depth and open-minded research project on the deployment of DLT. ASTRI delivered the first stage results of the project on 11 November 2016 with the publication of the *Whitepaper on Distributed Ledger Technology* (the first Whitepaper). The Whitepaper introduced the technology in detail and described three Proof-of-Concept (PoC) projects on which the HKMA had worked with ASTRI and five leading banks, namely Bank of China (Hong Kong) Limited, The Bank of East Asia Limited, Hang Seng Bank Limited, the Hongkong and Shanghai Banking Corporation Limited, and Standard Chartered Bank (Hong Kong) Limited[1], and their progress. It further reflected on a number of issues relating to governance, risk management, compliance, security and privacy, and legal matters that were identified during the PoC projects.

This second Whitepaper provides an update and overview of the development of DLT, and outlines lessons taken from the three PoC projects. It also suggests some key principles relating to issues of governance, control measures and security management for DLT, and describes common legal and compliance issues encountered when deploying DLT, along with some possible steps to address these issues.

Given the expertise required in many of these areas, the HKMA is pleased to have received professional input from Deloitte and PwC in relation to issues of governance, control measures and security management in the deployment of DLT. In addition, the HKMA has been honoured to receive professional contributions from The Law Society of Hong Kong along with academic input from law professors Dirk Zetzsche, Ross Buckley and Douglas Arner dealing with the privacy and legal issues identified. Finally, ASTRI has continued to provide assistance by preparing a technology update on the latest developments in DLT since November 2016.

Given the still evolving nature of DLT, it has not been possible for this second Whitepaper to uncover and describe all the implementation issues and address them fully. Rather, its purpose is to contribute to the growing body of knowledge on DLT, and to provide a window into the workings of DLT and an understanding of how it can benefit the banking and payment industry by reference to real-life PoC projects. Furthermore, the HKMA hopes that the issues identified from the PoC projects and the expert advice received will give confidence to those considering DLT deployment for specific applications, by making them aware of common factors/issues that need to be considered and the types of experts that need to be engaged. This will in turn enable developers to anticipate in good time any new issues that may surface in their specific areas.

2.2 Distributed ledger technology

Development of a number of platforms such as Hyperledger, Corda, Bitcoin and Ethereum is continuing. Recent developments include the formal release of Hyperledger and a new version of Corda, different suggested approaches for tackling the block size limit of Bitcoin, and a proposed proof-of-stake consensus algorithm to improve the performance of Ethereum. A number of players have been active in bringing unpermissioned DLT networks into enterprise operation. This has been achieved by, for example, modifying a public DLT network such as Ethereum into the permissioned Quorum, defining additional standards (as the Enterprise Ethereum Alliance has done) to provide privacy and performance assurances, and suggesting frameworks for governing how DLT would operate so as to conform to the needs of enterprises, as in the case of Microsoft. Performance and scalability remain major limiting factors for DLT, and a number of off-chain service technologies have surfaced as a result which are enabling the DLT processing burden to be offloaded.

[1] In alphabetical order

2.3 Compliance issues

Compliance is about identifying and managing risks often related to finance, operation, technology, governance and law, and meeting supervisory and legal requirements. While the topics covered by the term 'compliance' are fluid and in some cases overlap, a total of seven items have been identified as baseline compliance issues in this Whitepaper. They should provide a good starting point for those engaged in DLT design and deployment, helping developers avoid the need for after-the-fact, bolt-on compliance measures that may be costly and ineffective.

2.4 Governance, control principles and cybersecurity

A common theme running throughout the three PoC projects as they tested the implementation of DLT technology has been the issue of governance. As all the PoC projects deployed permissioned DLTs, establishing a governance structure and framework has been crucial for ensuring the viability of the DLT solutions.

Three approaches — consortium, joint venture, and separate organisation — have been proposed for the possible governance structure. Their advantages and disadvantages have been compared in terms of cost, flexibility, time needed for establishment, legal certainty, market recognition and level of controls. In terms of governance frameworks and controls, lengthy deliberations have been made for the benefit of potential practitioners on the available options and on best practice with regard to membership on-boarding procedures, the drafting of end-user agreements, data privacy controls, authentication and access controls, security administration and monitoring, system development, change management, portability and compatibility, disaster recovery and resilience.

Smart contracts have been singled out as requiring additional attention due to their huge potential for automating transactions in DLT.

Discussion around cybersecurity has not only included consideration of a range of 'traditional' security management techniques for physical, logical and network security. In addition, a number of techniques relating to key management have been discussed at length.

2.5 Legal Considerations

Legal issues also connect all three PoC projects, and require expert input and advice.

DLT solutions often involve replacing and automating laborious paperwork, so the legal basis on which such digitisation is carried out must be sound. While the exchange of digitised documents between private parties may be underpinned by agreements, checks should be carried out to ensure that there is a valid legal basis for the digitisation of documents that are definable under the law, such as title deeds, negotiable instruments, etc.

DLT solutions often involve the storage of personal data. The three characteristics of DLT of data transparency, immutability and cross-border implementation could raise concerns over the data protection principles of 'need-to-know', the right of deletion/correction, and the right or otherwise of the data user or controller to store collected personal data in another jurisdiction. A simple way of addressing these concerns is to store personal data off-chain, thus allowing participants more control over how personal data is handled and protected. This arrangement is particularly appealing in more complex cases where DLT solutions are subject to the data protection laws of multiple jurisdictions.

Although DLT solutions often operate across borders and give rise to legal issues relating to contractual and jurisdictional arrangements, such issues are not new in the world of global trade and there are established ways of handling them.

Given that smart contracts remain at an early stage of development, many legal issues potentially arising from them are yet to be fully understood and addressed in the legal system. That said, one important piece of advice is that smart contracts should not be considered as a complete replacement for formal legal relationships between parties. In other words, a traditional contract or agreement is still considered to be the best way of protecting all parties.

The governance structure of DLT solutions, which determines the level of control and participation of each party, has a significant effect on each party's level of liability. Participants must therefore study the terms and conditions or contracts carefully, and ensure they understand their implications before participating.

Competition law is relatively new in Hong Kong. To avoid getting themselves into uncharted territory, participants should take care that their use of DLT does not create an artificial or technological barrier that enables or facilitates a monopoly.

Finally, the Law Society has provided detailed discussion on the use of DLT in specific areas, including physical asset management, e-Conveyancing, trade finance and digital identity management, as examples of the legal considerations connected with specific types of applications. This is available in the Annex.

2.6 Proofs-of-Concept

The three PoC projects on trade finance, digital identity management and mortgage loan applications were chosen because these processes are often unstructured, manual and paper-based. They are labour intensive and time-consuming, involve multiple parties, and are prone to error and potential fraud. The use of DLT aims to enhance process and data transparency, trust between parties, data security, the traceability of transactions, and the efficiency and level of process standardisation.

For each PoC project, prototypes of DLT solutions were constructed and tested by participating banks. The processes and results were then reviewed and discussed in order to identify the associated benefits and challenges.

The diversity of the three PoC projects allowed participants to learn from real-world experience and identify common issues surrounding the deployment of DLT applications. For example, using a modular architecture to separate the DLT ledger from the workflow application and the interfaces used by participants, together with Application Programming Interfaces (API) to link them together, was soon found to be a necessity. Such modular design allows both new and existing participants to easily join the application, connect their disparate internal systems to the ledger, and make changes without affecting others. It was also agreed that the amount of information or documentation to be stored in the DLT ledger should be kept to a minimum for reasons of performance, flexibility and privacy protection.

Other common challenges facing the PoC groups included the difficult decision of which DLT platform to choose to build the prototype or production systems on. Given the development of a range of DLT platforms and the lack of standards, PoC participants struggled with this decision since they did not know the impact that future market developments, standardisation and interoperability might have. Another common challenge was the choice of a governance structure, as each PoC project had its own characteristics and business constraints that participants had to take into account.

Finally, all three project teams shared the view that many of the challenges and discussions they faced did not arise from the DLT technology itself, but rather from the associated issues of governance, controls, operation, maintenance and administration of the DLT platforms.

2.7 Ways Forward

The HKMA engaged in the three PoC projects in order to obtain first-hand experience of DLT, with the aim of understanding its advantages and disadvantages, particularly in those areas of its application that require solid data integrity.

More specifically, the trade finance PoC project is planned to progress into the Hong Kong Trade Finance Platform, using digitalised trade documents to automate the trade finance process, reduce the risk of duplicated trade finance and increase the financing capacity of the banking industry. The design will incorporate a “connectivity highway” for cross-border data exchange with other jurisdictions using similar trade platforms.

Apart from the PoC projects, the HKMA has also commenced research on Central Bank Digital Currency (CBDC) with the aim of assessing the potential benefits, challenges and future implications of issuing CBDC. This is another example of the growing potential for the application of DLT.

In conclusion, the HKMA has always adopted a risk-based, technology-neutral approach to regulation. Its goal is for the two Whitepapers to help the industry better understand the specific potential of DLT as well as related issues surrounding its implementation. Individual organisations deploying DLT must remember that they have a responsibility to strike the right balance between innovation, customer protection and risk management.

Chapter 3

Introduction

3.1 Background and history

In 2008 blockchain technology, a specific type of Distributed Ledger Technology (DLT), was conceptualised in a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System"[1]. The paper suggested how certain technologies existing at the time, such as decentralised peer-to-peer networks, asymmetric-key cryptography, hashing functions and Byzantine Fault Tolerance design, could be put together to form a blockchain. In January 2009, the first Bitcoin built on blockchain technology made its debut in "a system for electronic transactions without relying on trust"[2]. Since then blockchain, and more generally DLT, a 'disruptive technology' which enables a replicated and shared ledger system to be built that renders an intermediary redundant, has attracted much interest from the financial world.

In 2015 a variant of DLT was combined with a programming language to create the Ethereum platform, which allows participants to execute self-enforcing transactions as "smart contracts"[3]. Since then more and more unpermissioned/public platforms (e.g. Ethereum, Factrom, and Blockstream) and permissioned/private platforms (e.g. Hyperledger, Corda, Blockstack, Multichain, and Chain Inc.) have been launched to meet different needs. Growing interest in the technology has led financial institutions to announce plans to explore the possibilities of DLT beyond the field of cryptocurrencies.

Against this background, the Hong Kong Monetary Authority (HKMA) commissioned the Hong Kong Applied Science and Technology Research Institute (ASTRI) to undertake an in-depth, open-minded research analysis into the deployment of DLT, especially for financial applications. ASTRI delivered the first stage results of the project on 11 November 2016 with the publication of the *Whitepaper on Distributed Ledger Technology* (the first Whitepaper). The first Whitepaper described the technical building blocks of DLT, its modes of operation, its performance, and its disruptive properties and interoperability. The first Whitepaper outlined the features of the various DLT platforms available at the time, and how they differed from each other. It also presented details of the three Proof-of-Concept (PoC) projects on which the HKMA was working with ASTRI and five leading banks, namely Bank of China (Hong Kong) Limited, The Bank of East Asia Limited, Hang Seng Bank Limited, the Hongkong and Shanghai Banking Corporation Limited, and Standard Chartered Bank (Hong Kong) Limited[4], and described their progress. It further deliberated on various issues relating to governance, risk management, compliance, security and privacy, and the law which were identified during the various PoC projects — these are all issues that need to be adequately addressed if DLT is to be applied to critical financial applications.

3.2 Purpose and scope of the second Whitepaper

The HKMA is publishing this second Whitepaper as a follow-up based on its further research into DLT. The three PoC projects have been completed and various lessons taken from them. To address the governance, compliance and security issues identified, the HKMA sought professional contributions from Deloitte and PwC. In addition, the HKMA is honoured to receive contributions from The Law Society of Hong Kong and from law professors Dirk Zetzsche, Ross Buckley and Douglas Arner in relation to the privacy and legal issues identified. Finally, ASTRI has also provided assistance by preparing a technology update on the latest developments in DLT since the first Whitepaper was published.

Building on these expert contributions, this second Whitepaper aims to provide an update and overview of the development of DLT, describe the lessons taken from the three PoC projects, suggest some key principles concerning governance, controls and security management, and describe a number of legal and compliance issues encountered in the deployment of DLT along with possible steps to address these issues.

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] Ibid.

[3] Smart contracts can be defined as automated transactions based on pre-defined events.

[4] In alphabetical order.

Given the still evolving nature of DLT, the diverse possibilities for its application, and the evolving experience of those who are actively exploring the use and potential of DLT in their fields, it has not been possible for this second Whitepaper to pinpoint all the implementation issues and address them fully. Rather, its purpose is to provide readers with a window into the workings of DLT and to describe some of the benefits offered by DLT to the banking and payment industry, through reference to real-life PoC projects. Furthermore, the issues that have been identified in the PoC projects and discussed in the expert advice received will help those who are interested in implementing DLT but are concerned about possible pitfalls. This Whitepaper can help build confidence by clarifying the range of common factors/issues that need to be considered and the types of experts that need to be engaged. This may also help developers anticipate in good time any new issues that may surface in their specific areas of application.

3.3 Structure of the second Whitepaper

The rest of this Whitepaper provides overviews and summaries of developments in DLT, governance, compliance and legal issues arising from DLT, and insights taken from the three PoC projects.

Original expert contributions are included as separate Annexes, providing in-depth analyses of specific topics.

More specifically, Chapter 4 provides an overview of the latest developments in DLT and further expected developments in the future. Chapter 5 introduces a range of compliance issues that need to be considered when deploying DLT applications. Chapter 6 provides a more in-depth discussion on the topics of governance, control principles, and security and cybersecurity management. Chapter 7 deliberates on a range of legal issues that may arise. Finally, Chapter 8 describes the three PoC projects on trade finance, digital identity management and mortgage loan applications, and the lessons taken from them.

3.4 Ways forward

Many central banks and regulators have published papers on DLT and its application. Recognising the potential of DLT, the HKMA is contributing by engaging in PoC projects to obtain first-hand experience, and sharing details of these in the two Whitepapers. Like most technologies, DLT has its advantages and disadvantages. There are specific areas where its application may be especially beneficial, particularly those that require solid data integrity.

Five banks are moving forward with the trade finance PoC project. They are working on implementing a Hong Kong Trade Finance Platform that will use digitalised paper-based trade documents to automate the trade finance process, reduce the risk of duplicated trade finance, and increase the financing capacity of the banking industry. The design will incorporate a “connectivity highway” for cross-border data exchange with other jurisdictions using similar trade platforms.

Apart from the PoC projects, the HKMA has also commenced research to explore the potential of DLT for Central Bank Digital Currency (CBDC) with the three note-issuing banks, the Hong Kong Interbank Clearing Limited and the R3 consortium. This research aims to assess the potential benefits, challenges and implications of issuing CBDC, and represents another way forward for the potential use of DLT within the financial industry.

The HKMA has always adopted a risk-based, technology-neutral approach to regulation. This being so, we wish to point out that the issues identified in these two Whitepapers are not exhaustive, and any suggestions offered are for guidance only. Those deploying DLT applications must make their own assessments and judgements regarding compliance issues with the aim of striking the right balance between innovation, customer protection and risk management.

Chapter 4

Technology Update

Chapter 3 of the first Whitepaper gives an introduction of DLT. It is followed by Chapter 4 with in-depth details on the technology and security design. Chapter 6 of the first Whitepaper also describes the features of various DLT platforms available. As a follow-up, the HKMA has sought help from its strategic partner, ASTRI, to provide an update in this second Whitepaper on the recent developments of the technology. The remaining part of this chapter is contributed by ASTRI.

4.0 DLT Technology: Maturing towards production

As blockchain technology continues to gain acceptance, a growing number of individuals and businesses are using the technology for cryptocurrency transactions and smart contract applications. At the same time, various DLT Proof-of-Concept projects have been carried out to evaluate the benefits and the capabilities of DLT technologies for a wide spectrum of other applications. DLT technology developers are now setting their sights on full production. As a result, many development activities are now taking place that are focused on enhancing the technology in areas such as transaction processing performance, privacy protection, and versatility.

4.1 DLT Platforms

4.1.1 Hyperledger

Hyperledger is an open source blockchain technology hosted by The Linux Foundation. It represents a global collaboration between members of many different industries, including finance, banking, the Internet of Things, supply chain, manufacturing and technology[1].

4.1.1.1 Formal release of Hyperledger Fabric Version 1.0

Hyperledger announced the formal release of its Fabric blockchain on 11 July 2017[2], following several pre-releases. The announcement stated that Fabric 1.0 is a robust major release that aims at allowing consumers and vendors to use Hyperledger Fabric technology to advance to production deployment and operations.

The pre-releases and formal release included documentation improvements, testing, hardening, bug fixing and tooling[3]. UX (user experience) improvements were also introduced based on user feedback.

4.1.1.2 Performance and robustness enhancement of Fabric

The Fabric version 1.0 release announcement indicated that Hyperledger's developer will continue seeking to enhance performance. There are also plans to improve the robustness of Fabric by running performance, scale and chaotic testing.

Part of the performance enhancement concerns transaction ordering based on the Byzantine Fault Tolerant algorithm. Ordering of transactions in Hyperledger is determined by a distributed set of special nodes called "orderers". Together they implement an ordering service that provides a "guarantee of delivery", e.g. a guarantee of atomic broadcast. The strength of the algorithm is that it can tolerate failure or misbehaviour by some of the orderers without affecting the reliability of the ordering service operation[4].

There are plans to explore the possibility of integrating Fabric with other Hyperledger projects such as Sawtooth. Sawtooth is an example of DLT which uses a consensus algorithm called "Proof of Elapsed Time" (PoET). Compared to the Proof-of-

[1] See "https://www.hyperledger.org/about"

[2] See "https://www.hyperledger.org/blog/2017/07/11/hyperledger-fabric-1-0-is-released"

[3] See "http://hyperledger-fabric.readthedocs.io/en/latest/releases.html"

[4] See "http://hyperledger-fabric.readthedocs.io/en/latest/arch-deep-dive.html"

Work (PoW) consensus, PoET operations consume a significantly lower amount of computational resources. This is achieved by secure CPU instructions in the hardware.

As Fabric is a DLT network for smart contract execution in which smart contracts, termed chaincode, are written in computer language, the versatility and security of the computer language is very important. Fabric's default smart contract language is Golang. Fabric plans to add Java and other programming languages to its list of chaincode development languages. According to the version 1.0.0-beta release notes of 8 June 2017, Java chaincode support has been disabled until a later version, when the feature has fully matured[5]. However, Java chaincode can currently be re-enabled for experimental purposes.

4.1.1.3 Blockchain technology spawned by Hyperledger

As the Hyperledger technology matures, businesses are beginning to build new technologies and services upon it. Fujitsu Laboratories Ltd has announced its development of technology that accelerates the speed of Hyperledger Fabric transaction processing by approximately 2.7 times its current speed in version 0.6.1[6]. The source of the bottleneck in Hyperledger was identified as being the communication between the application and the blockchain platform. The new technology resolves this bottleneck by introducing two features:

- Differential Update State (DUS) Functionality

  This eliminates some of the steps involved in processing a transaction that involve unnecessary communication between the application and the blockchain platform. For example, if an application desires to decrease the value of an asset on a blockchain platform, the old way of doing this was to have the application first retrieve the asset value from the blockchain platform, then decrease the value and write it back to the blockchain platform. With DUS, the application simply sends a differential computation instruction to the blockchain platform asking it to perform the decrement operation directly, thus reducing the number of communication exchanges and the associated computations.

- Compound Request (CR) Functionality

  This reduces the amount of communication between the application and the blockchain platform by aggregating multiple processes into a single batch execution request, which is then sent to the blockchain platform. One example is if the application is performing an asset transfer between two accounts. Instead of sending multiple instructions to the blockchain platform (one to decrease the asset value of the paying account and another to increase the asset value of the receiving account), the application simply sends a single batch execution request to the blockchain platform asking it to perform both actions.

A press release of 31 July 2017 indicates that Fujitsu Laboratories Ltd plans to commercialise this technology in the fiscal year 2017.

4.1.2 Corda

Corda is open source blockchain technology developed by R3. In 2017, R3 has continued with its development and enhancement of Corda, a distributed ledger platform for financial and commercial transactions. A 3 May 2017 press release noted, "Financial technology innovator R3 has completed the first two of three tranches in its Series A fundraising round, securing USD 107 million in the world's largest distributed ledger technology (DLT) investment to date." [7] R3 is continuing to release newer versions of the Corda platform.

4.1.2.1 The design of Corda

R3's David Rutter, in a 24 February 2017 blog article, reiterated the relationship between Corda and blockchain. He writes, "Corda is a distributed ledger

[5] See "https://github.com/hyperledger/fabric/releases/tag/v1.0.0-beta"

[6] See "http://www.fujitsu.com/global/about/resources/news/press-releases/2017/0731-01.html"

[7] See "https://www.corda.net/wp-content/uploads/2017/05/R3FundingPressRelease.pdf"

platform, not a traditional blockchain platform."[8] The article further clarifies, "Blockchains are specific pieces of software originally built to handle transactions of virtual currencies such as Bitcoin and Ether. Together with our bank members, we realised early on that this technology could not be applied blindly to wholesale financial markets without careful consideration: changes must be made to satisfy regulatory, privacy and scalability concerns. And that is what we have done with Corda."

The article also clarifies, "Corda restricts access to data within an agreement to only those explicitly entitled to it, rather than the entire network. And financial agreements on Corda are intended to be enforceable, linking business logic and data to associated legal prose in order to ensure that the financial agreements on the platform are rooted firmly in law."

4.1.2.2 The Corda platform releases

Corda announced the release of Corda Beta in June 2017[9,10]. According to its announcement, Corda has made substantial improvements to the performance of RPC (Remote Procedure Calls). On the security side, Corda now supports the use of hardware security modules (HSMs) for key storage, and can now support transaction signing without the need to extract private signing keys from the HSM. Corda also supports multiple signature schemes, and not just EdDSA (the Edwards-curve Digital Signature Algorithm). As for Corda Milestone 13, the digital signature algorithms that are supported include ECDSA secp256K1, ECDSA secp256R1 (NIST P-256) and EdDSA ed25519.

On 3 Oct 2017, R3 announced the release of version 1.0 Corda. This marks a major milestone for the development and implementation of applications on the platform, known as CorDapps. One major achievement in this release is the stabilisation of application programming interface (API) used by CorDapps. Developers may now develop CorDapps with the knowledge that they will be compatible with future Corda platform releases.[11]

4.1.2.3 Corda Support

In an announcement of 29 June 2017[12], it was stated that Corda would soon launch a service named Corda Support. This would be an enterprise-grade support service for Corda implementation to support enterprises looking to deploy Corda for production, by providing professional assistance.

4.1.3 Bitcoin

The transaction volumes of Bitcoin have risen rapidly in the past few years, from a daily volume of around 100,000 transactions in 2015 to a peak of over 350,000 transactions in 2017[13]. Different strategies have been proposed to increase Bitcoin's transaction processing capacity. The Bitcoin community, including both miners and users, are the ones that will ultimately decide on the proposal to be accepted.

4.1.3.1 Bitcoin Segregated Witness proposal

This proposal introduces a concept called Segregated Witness (SegWit), which brings with it multiple benefits. Among these are increased block size and transaction malleability protection. The current Bitcoin protocol adds transactions (comprising transaction details and transaction signer signatures) to the transaction Merkle tree to form a block. These blocks are then linked up to form the blockchain. The proposal introduces the SegWit concept and a new structure called "witness" for storing signatures and relevant scripts. These signatures and scripts are originally stored in the transaction structure in the block. They will now be separated and stored in the "witness" structure, hence the term SegWit, which stands for Segregated Witness. The witness structure is committed to a new tree. In the initial implementation, this tree will be linked to the block's transaction Merkle tree through the block's coinbase transaction[14].

[8] See "http://www.r3cev.com/blog/2017/2/24/when-is-a-blockchain-not-a-blockchain"

[9] See "https://www.corda.net/2017/06/announcing-corda-public-beta/"

[10] See "https://www.corda.net/2017/06/corda-beta-released/"

[11] See "https://www.r3.com/blog/2017/10/03/r3-launches-version-1-0-of-corda-distributed-ledger-platform/"

[12] See "https://www.corda.net/2017/06/corda-support-available-soon/"

[13] See "https://blockchain.info/charts/n-transactions?timespan=all"

[14] See "https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki"

Thus, the transmission of a signature becomes optional, and is not needed if a user is simply checking the existence of a transaction. This reduces overheads for lightweight wallets in terms of both processing time and storage.

The current block size limit of 1 Megabyte will be increased with Segregated Witness. The proposal introduces a parameter called Transaction Weight to set the total size of transactions permissible in a block. The total size depends on the amount of segregated witness data in the transactions inside the block. Transactions using the segregated witness feature will be accommodated with a bigger block size.

There are other benefits of this proposal, such as linear scaling of sighash operations and increased security for multisig via pay-to-script-hash (P2SH)[15].

4.1.3.2 Bitcoin Unlimited

Bitcoin Unlimited makes a small change to the consensus in the Bitcoin core, so that the consensus no longer enforces a hardcoded block size limit. The maximum size of a block is freely adjustable by miners, who then engage in Emergent Consensus (EC) to set the maximum block size. Initially different miners may set their own maximum block size limit to different values (called Excessive Blocksize), and delay their acceptance of any block over that size. If a miner raises its Excessive Blocksize value, generates a block of that size and sends it to the network, it is left to all the other nodes to decide whether to accept this block based on their own Excessive Blocksize values. If the block's size does not exceed the Excessive Blocksize value setting of the receiving node, the node will accept it and will build future blocks on top of it. On the other hand, if the block size exceeds the Excessive Blocksize setting of the receiving node, the node will postpone accepting this oversized block until the block has reached a certain block depth (called Acceptance Depth, or AD), meaning that the receiving node sees that the prevailing, or longest chain, has incorporated this block and has appended the required number of new blocks to it[16].

Bitcoin Unlimited also introduces other technologies such as Extreme Thin Blocks (Xthin), Xpedited Forwarding, and Traffic Shaper.

4.1.3.3 Bitcoin Cash

Bitcoin Cash (BCC) takes another approach and provides an immediate increase of the block size limit to 8 Megabytes. Bitcoin Cash also introduces other changes such as Replay Protection and Wipeout Protection[17].

Replay refers to an attack on the blockchain that could occur if a blockchain has forked into two, made up of the original blockchain and a new blockchain. The Bitcoin owner now can spend a coin twice, once in each of the two blockchains. If the owner of the cryptocurrency sends a transaction to the original blockchain to spend the coin, an attacker could capture the transaction and send it — in other words, replay it — to the new blockchain. While the attacker might not benefit from the attack, the owner no longer owns the coin in the new blockchain even though he has not spent it in that blockchain. Bitcoin Cash Replay Protection seeks to prevent this from happening.

Bitcoin Cash also introduces a new way of signing transactions as part of the replay protection technology. This involves defining a new SigHash type, and it brings the benefits of improved hardware wallet security and elimination of the quadratic hashing problem[18]. SigHash is a Bitcoin signature flag indicating which part of the transaction is signed by the signature[19].

[15] See "https://bitcoincore.org/en/2016/01/26/segwit-benefits/"

[16] See "https://www.bitcoinunlimited.info/faq/what-is-bu"

[17] See "https://news.bitcoin.com/what-every-bitcoiner-should-know-about-bitcoin-cash/"

[18] See "https://www.bitcoincash.org/"

[19] See "https://bitcoin.org/en/glossary/signature-hash"

4.1.4 Ethereum

There has been a similar demand for Ethereum to raise its transaction processing rate. Recent examples of ICO (Initial Coin Offering) activities on the Ethereum platform have demonstrated such a need, with investors sending a large number of transactions to Ethereum to make their investments.

4.1.4.1 Proof-of-stake

Ethereum developers are designing a Proof-of-Stake consensus algorithm called Casper[20]. The traditional consensus of Ethereum is proof-of-work, which requires a large amount of electricity for miners to generate the blocks. Proof-of-Stake seeks to reduce electricity consumption. In the case of Ethereum, the consensus will be security-deposit based. Miners that have paid the security deposit become bonded validators and are entitled to take part in generating blocks through the consensus process.

With proof-of-stake mining, the Casper blockchain will also be able to create more blocks than the current proof-of-work mining can.

The developers are gradually revealing the migration path to Casper proof-of-stake[21]. A "Casper Version 1 Implementation Guide" document published on 7 May 2017 indicates that Ethereum will first transition from pure proof-of-work to a proof-of-work/proof-of-stake hybrid model. [22] In this hybrid model, proof-of-work will still be used for generating blocks. However, every 100th block in the blockchain will be designated as a checkpoint. Proof-of-stake consensus will then be applied to finalise this checkpoint block. A finalised checkpoint block marks the point from which there is no going back to undo the previous blocks. The document also discusses methods for conflict resolution.

4.1.4.2 Other planned Ethereum enhancements

According to a recent interview with Vitalik Buterin, the co-founder of Ethereum, Ethereum wants to continue enhancing quite a number of areas, including privacy, scaling, and sharding[23].

4.2 Unpermissioned DLT technology extension for enterprises

Since some unpermissioned DLT platforms are rich in features and are relatively stable and mature, business sectors have begun to contemplate extending them to support their enterprise operations. Such extension includes introducing features and capabilities to the DLT platforms to address the specific needs of enterprise operations, such as the preservation of privacy, controls over membership, and the need for high transaction rates.

4.2.1 Quorum

Quorum is a permissioned DLT platform developed by JP Morgan. It is based on a modification of Ethereum designed to serve enterprise applications. Such applications do not simply include financial applications. Quorum brands itself as having the capability to process private transactions at high speeds, and with high throughput.

Quorum provides both the privacy and the transparency often desired. While transaction privacy is required by the financial industry, system and network transparency is also desirable for the transacting partners to ensure consistency. Quorum is also designed to be customisable to meet the differing requirements of various business applications.

These benefits are achieved as follows[24]:

- All public and private smart contracts and the overall system state are derived from a single, shared, complete blockchain of transactions validated by every node in the network.

[20] See "https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/"

[21] See "https://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake/"

[22] See "https://github.com/ethereum/research/wiki/Casper-Version-1-Implementation-Guide"

[23] See "https://bitcoinmagazine.com/articles/interview-vitalik-buterin-ethereum-scaling-issues-popularity-asia-and-icos/"

[24] See "https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf"

- A private smart contract state is only known to and validated by parties to the contract and approved third parties, such as regulators.

- The list of transactions is validated by all nodes, but only relevant parties have access to details of the private transactions and contracts.

Quorum emphasises its code maturity. JP Morgan has stated, "Quorum is designed to develop and evolve alongside Ethereum. Because it only minimally modifies Ethereum's core, Quorum is able to incorporate the majority of Ethereum updates quickly and seamlessly." [25]

4.2.1.1 Zero-knowledge security layer

In a 22 May 2017 press release, Zerocoin Electric Coin Company, the developer of Zcash, announced that Zcash technology will be incorporated into Quorum[26]. The technology creates a cryptographically enabled zero-knowledge security layer. It extends the ability of Quorum to protect the privacy of business transactions in a DLT platform with no central intermediaries.

The technology applies zero-knowledge cryptography and introduces a new methodology for transaction structures and validation. With the technology, transactions can be validated without revealing the details of the origins, destinations, or amounts of payments made. For example, the technology allows a party to perform computation on a set of parameters, and produces a statement of the computation results. It then passes the statement to a third party and tells it that it is true. This third party may then verify that the statement is true, without knowing the parameter details. This is generally known as zero-knowledge proof. zk-SNARKs is a well-known example of the zero-knowledge cryptography used by Zcash[27]. Its full name is "zero-knowledge succinct non-interactive arguments of knowledge"[28]. Among the ingredients of zk-SNARKs is homomorphic encryption, which allows computation to be performed on encrypted data without its plain data value being known. The result, when decrypted, is identical with the result from the same computation performed on the plain data.

4.2.2 Enterprise Ethereum Alliance

The Enterprise Ethereum Alliance has recently received industry attention. It is an alliance with a broad membership, and includes Fortune 500 enterprises, start-ups, academics, and technical vendors. It aims to utilise Ethereum to build enterprise-grade software capable of handling complex software with high performance requirements. A 7 July 2017 press release[29] reiterates its mission thus: "EEA is a non-profit industry organisation that defines standards so applications built on an Ethereum-derived platform will run on all Ethereum platforms as well as supporting the development of enterprise tools and support."

The Alliance also announced its support for pluggable consensus algorithms, and its first integration of the Practical Byzantine Fault Tolerant (PBFT) consensus with JP Morgan's Quorum blockchain platform.

To enable Ethereum to support enterprise applications, the Alliance will focus on privacy and performance improvements[30]. It indicates it will continue to commit to providing open source, free-to-use blockchain solutions.

Membership of the Enterprise Ethereum Alliance continues to grow, with members coming from various sectors. Current members include Microsoft, Cisco, Intel, Mastercard, Thomson Reuters, UBS, Monax, and Accenture.

4.2.3 Microsoft Enterprise DLT Framework

Instead of focusing on designing a new blockchain for enterprise applications, Microsoft has introduced a framework for adopting different popular permissioned/unpermissioned DLT platforms. The

[25] See "https://www.jpmorgan.com/country/US/EN/Quorum"

[26] See "https://z.cash/blog/zsl-quorum.html"

[27] See "https://github.com/zcash/zips/blob/master/protocol/protocol.pdf"

[28] See "http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf"

[29] See "https://entethalliance.org/enterprise-ethereum-alliance-announces-support-blockchain-consensus-algorithm-integration/"

[30] See "https://entethalliance.org/"

framework provides both basic groundwork and features to enhance the security and performance of the DLT services, making them suitable for enterprise applications.

4.2.3.1 Project Bletchley

Bletchley is a cloud-based Enterprise blockchain architecture framework from Microsoft. The framework does not introduce a new blockchain protocol or stack. Instead, it is to be an "Enterprise Consortium Distributed Ledger Fabric" with the purpose of integrating blockchain platforms and related technologies to deliver enterprise-grade services[31].

To achieve this, Bletchley adopts a modular design to enable easy integration of different technologies into the framework. Among such technologies are blockchain protocols, consensus algorithms, databases, and virtual machines.

The Bletchley framework provides a set of core services. Various blockchain stacks may then be plugged into the base of the framework, called the Base Platform Tier. Applications run at the top of the framework. The Bletchley core services sit in the middle between the applications at the top and the blockchain stacks at the bottom. Hence, the core services act as the middleware.

Bletchley core services include:

- Identity and Certificate Services
- Encryption Services
- Cryptlet Services
- Blockchain Gateway Services
- Data Services
- Management and Operation

According to the Bletchley whitepaper, the Base Platform Tier supports Smart Contract type blockchains such as Ethereum and Eris (now also known as Monax), and UTXO type blockchains such as Hyperledger.

4.2.3.2 Coco

Microsoft announced on 10 Aug 2017 its new enterprise blockchain platform called the Coco framework[32]. This aims to reduce the complexity of the development techniques needed for current blockchain technologies to meet the operational and security requirements of enterprises. It is designed to address the needs for high transaction speeds, distributed governance and confidentiality.

The press release lays out the key benefits as follows:

- Transaction speeds of more than 1,600 transactions per second
- Easily managed data confidentiality without sacrificing performance
- A comprehensive, industry-first distributed governance model for blockchain networks that establishes a network constitution and allows members to vote on all terms and conditions governing the consortium and the blockchain software system

Coco is designed to be compatible with any blockchain protocol and can be operated in different settings, such as on-cloud or on-premises. The initial Coco framework will include R3's Corda, Intel's Hyperledger Sawtooth, JP Morgan's Quorum, and Ethereum.

The many benefits of Coco are based on the element of Trusted Execution Environments (TEEs)[33]. TEE is a secure area of a processor where code is executed. Data and code within a TEE is protected, offering confidentiality and uncorrupted integrity. Examples of TEEs are Intel's SGX and the Windows Virtual Secure Mode (VSM). TEE enables the building of a trusted network for running enterprise blockchain. TEE serves as an enclave containing the Coco core and configuration state information, the adapted blockchain core, and the replicated persistent store. The use of TEE will help improve blockchain

[31] See "https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md"

[32] See "https://news.microsoft.com/2017/08/10/microsoft-announces-the-coco-framework/"

[33] See "https://github.com/Azure/coco-framework/blob/master/docs/Coco%20Framework%20whitepaper.pdf"

transaction performance by reducing the consensus problem of Byzantine Fault Tolerance to crash fault tolerance. And because the code execution in TEE is trusted, a smart contract needs only be executed by a single node in the network. The trusted nature of TEE enables systems to reduce electricity consumption by not having to use computationally intensive proof-of-work consensus.

Microsoft plans to launch the Coco framework as an open source project in 2018.

4.3 Off-chain services technology for DLT

While popular DLT platforms are secured by cryptographic protection, their growing popularity and the resulting traffic are placing a strain on their performance. Examples of such DLT platforms are Bitcoin (as a cryptocurrency) and Ethereum (as an ICO vehicle). All are hard-pressed to increase their transaction processing rate. To dramatically improve their performance, one approach is to add off-chain services to these DLTs. The technology allows off-chain services to pick up a significant part of the transaction processing load on behalf of the DLT, and hence reduces the DLT processing load. Since off-chain processing can be conducted at a higher speed, the overall transaction volume also increases. Off-chain services are conducted in a secure manner, with their transaction processing results passed to the DLT for final validation and incorporation into the blockchain.

4.3.1 Lightning Network on Bitcoin

The Bitcoin network is reliable and Bitcoin has become widely used as a payment cryptocurrency. The Lightning Network is designed to extend the use of Bitcoin into new areas such as rapid and low-cost payments[34]. In addition, it is helping the Bitcoin system to scale more efficiently as a global payment processing system.

In a Lightning Network, multiple payment transactions between trading partners may be conducted off the chain. Only the final settlement balance is recorded in the blockchain, thus reducing the DLT transaction processing burden. Another benefit is better privacy protection. Having transactions on the Lightning Network conducted between trading partners and without exposure to external parties, and having only the final transaction outcome recorded to the Bitcoin blockchain, means a higher level of transaction privacy can be achieved.

The Lightning Network is a service built on top of the Bitcoin blockchain[35]. Through cryptographic technology, transactions may be conducted on the Lightning Network securely and quickly, not subject to the 10-minute mining period restriction of the Bitcoin network. All such transactions are nevertheless conducted in Bitcoin cryptocurrency, and the transactions are eventually combined and immutably committed to the Bitcoin blockchain.

The Lightning Network applies cryptographic technology to assure users that their off-chain processed transactions are guaranteed to be enforceable on the blockchain. The technology involves concepts such as multiple signature, Hashed Timelock Contract (HTLC)[36] and CheckLockTimeVerify (CLTV)[37]. HTLC uses the cryptographic hash to enable payment across multiple parties, and even across multiple blockchains. CLTV provides the ability to restrict the creation of transactions so that they are valid only after a certain point of time. Its verification capability also enables transactions to be constructed in such a way that different actions are conditionally enabled based on the time. For example, a transaction may be constructed in such a way that it is spendable only if both Alice and Bob have signed to spend it. However, the transaction may use CLTV to specify that, after a certain period of time, only Alice's signature is required to spend it.

[34] See "https://lightning.network/lightning-network-summary.pdf"

[35] See "https://en.bitcoin.it/wiki/Lightning_Network"

[36] See "https://lightning.network/lightning-network-paper.pdf"

[37] See "https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki"

The Lightning Network is suitable for applications such as micropayments and instant payments, transactions which occur frequently and for which users are only willing to pay a low transaction fee. It is also suitable for machine-to-machine payments.

The Lightning Network is built using features from Bitcoin Segregated Witness. The alpha version of the Lightning Network node implementation, called Lightning Network Daemon, was announced in early 2017[38]. Development is continuing, and several alpha release versions have been made available since then[39].

4.3.2 The Raiden Network on Ethereum

Like the Bitcoin Lightning Network, the Raiden Network is a layer added on top of Ethereum. It behaves as an off-chain network for Ethereum, and delivers certain desirable extra features. Transactions are conducted on it and are confirmed and finalised within a fraction of a second. While individual transactions are not stored in Ethereum, the final outcome is committed to Ethereum as the ultimate proof. Raiden aims to bring the following benefits[40]:

- Scalability according to the size of participants
- Fast transaction confirmation
- Transaction confidentiality
- Interoperability with tokens that conform to Ethereum's standard token API
- Low fees

The low fees offered by Raiden make micropayment feasible. This in turn enables other applications that are transacted with micropayments. One example is video streaming, where viewing is charged by the second. Another example is IoT resource sharing, where services offered are measured in small units such as (for example) storage space sharing and CPU time sharing.

The Raiden Network enables Ethereum to scale in terms of overall transaction volume, and is currently under development.

4.3.3 Plasma on Ethereum

On 11 August 2017, a working draft of the Plasma framework was released[41]. It was co-authored by Vitalik Buterin and Joseph Poon, who is also a co-author of the Lightning Network whitepaper. The framework aims to enhance the scalability of smart contract execution so that potentially billions of smart contract state updates may be performed every second.

The Plasma framework defines the concept of a parent blockchain and child blockchains, with blockchains arranged in a tree hierarchy. At the root of the tree is the root blockchain. Ledger entries are added to the child blockchain. The root blockchain, e.g. Ethereum, will ultimately enforce transaction state changes for all smart contracts. There can be many child blockchains existing simultaneously, each with its own business logic and smart contract terms, e.g. micropayments and decentralised exchanges. Much of the computation for smart contract processing is done on a child blockchain, with the computation results ultimately passed to the parent blockchain for enforcement.

In the Plasma framework, blockchain computations are reframed into a set of functions called MapReduce. MapReduce computations on a child blockchain are committed to Merkle proofs, for effective verification, which are then enforced on the parent blockchain through a mechanism called fraud proof. The process continues until the enforcement reaches the root blockchain. Fraud proof ensures that all state transitions are valid. Participants creating fraudulent blocks will be penalised.

[38] See "https://www.cryptocoinsnews.com/bitcoin-scaling-solution-lightning-network-releases-milestone-implementation/"

[39] See "https://github.com/lightningnetwork/lnd"

[40] See "http://raiden.network/"

[41] See "http://plasma.io/plasma.pdf"

Chapter 5

Compliance Issues

5.1 Background

“Compliance issues” is a loose term that can cover a range of concerns, including financial risk, operational risk (including technology and cybersecurity risk), governance, and legal matters. These issues may be broadly summarised into the following areas, each of which is particularly relevant to any DLT implementation:

1. Anti-money laundering and counter-financing of terrorism issues
2. Systemic risk
3. Technology and operational risks
4. Reporting and transparency
5. Governance and controls
6. Cybersecurity
7. Legal issues

This list is not exhaustive and could certainly be expanded depending on the actual purposes, circumstances and functions of any DLT application. Because the technologies and practices related to DLT are still evolving and the associated risks have not yet been adequately identified and understood, there is currently no specific regulatory guidance on DLT implementation. The issues identified in this chapter cannot therefore be considered as regulatory issues to be addressed. However, the chapter can still serve as a starting point for identifying the typical range of risks that need to be considered and addressed when designing and deploying DLT solutions. It should also be noted that there is no formal standard for categorising these items and determining their scopes, and it is quite acceptable that some scopes may overlap. Financial risks and operational risks unrelated to the use of DLT are outside the scope of this analysis, as they are specific to the types of financial applications being used.

5.2 Anti-money laundering (AML) and counter-financing of terrorism (CFT) issues

Given concerns over the misuse of the global financial system to facilitate money laundering (ML), terrorist financing (TF) and other criminal activities, legal and regulatory AML/CFT requirements have been established as part of a global framework of measures assessed against international standards. These include customer due diligence and ongoing monitoring to ensure that the identities of customers of a financial institution[1], whether individuals or legal entities, have been properly identified, verified and regularly reviewed, and that relevant records of financial transactions are maintained and can be made available to competent authorities.

Against this backdrop of tightened standards and regulatory scrutiny, the global trend of financial institutions in their AML/CFT work has been one of minimising risk. Implementing more complex emerging technologies such as DLT will require considerable innovation and internal technology capabilities on the part of financial institutions, and they will need to demonstrate the ability to truly understand and operate these technologies and mitigate any perceived ML/TF risks. While there is no specific AML/CFT regulation which precludes financial institutions from using DLT, there are nevertheless wide-ranging AML/CFT regulations requiring financial institutions to put in place proper measures, systems and controls to mitigate any ML/TF risks arising from their operations. Financial institutions may be uncertain of the suitability of unproven technologies such as DLT to meet these obligations. Also, a recent UK study[2] suggests that financial institutions have a clear preference for adopting proven technologies wherever possible. The risk of

[1] In Hong Kong, the CDD and record-keeping requirements are applicable to the financial institutions defined under Part 2 of Schedule 1 to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap 615).

[2] “New Technologies and Anti-Money Laundering Compliance”, UK Financial Conduct Authority, 31 March 2017

using unproven, non-regulator approved or endorsed technologies like unpermissioned DLT platforms may thus be considered too high, particularly given that questions regarding the anonymity of participants have not been resolved and therefore use of an unpermissioned DLT platform as a mainstream financial application could potentially expose a financial institution using the application to substantial ML/TF risks.

With respect to a permissioned DLT platform, the designs of a governance structure covering criteria for customer on-boarding and a transaction monitoring system need to take into account relevant AML/CFT legal and regulatory requirements applicable to financial institutions. Details of the relevant governance and controls for a DLT platform are set out in Chapter 6.

5.3 Systemic risk

Systemic risk is the risk of a collapse or breakdown of an entire system. This could be caused by failure of the technology, the failure of one or more major participants, a series of fraudulent or illegal activities, or a major cyber attack. It could also be the result of a major operational or network failure.

DLT is still in the early stages of development, and there are a number of competing DLT platforms offering varying features and having different characteristics. Whether the market is sufficiently large to sustain all these platforms is unknown, but there is a high likelihood that certain DLT platforms will not survive in the future. The effects of discontinuing a DLT platform on one or more participating institutions that have invested substantively in it could be serious, and need to be considered by all institutions that are currently planning to deploy DLT solutions.

Similarly, DLT standards are still evolving. Those who deploy a DLT solution without a standard having been established run the risk of having to upgrade to another compliant version of the DLT once a standard has been established. This will involve extra costs and effort associated with learning about the differences, finding the relevant technical talent, and developing and testing a new system. In extreme cases, users may find themselves being left with a non-compliant version of the DLT platform that may cause interoperability and support issues in the longer term. These are all issues relating to DLT standards that need to be examined before any DLT solution is deployed. At the least, there needs to be awareness of the impact of standardisation on DLT solutions, and measures in place to track the drafting of standards and to ascertain the compatibility of the different DLT platforms and assess their future roadmaps.

Another source of systemic risk for DLT is its reliance on an encryption standard called PKI infrastructure. The protection could be undermined if fraudsters gain the computing powers needed to crack the keys (for example, through the use of very powerful or quantum computers, or similar techniques). If this were to happen when DLT was being widely used by the banking sector, and the encryption method could not be upgraded or was not quantum computer-proof, the level of systemic risk could be significant.

Some DLT platforms, notably unpermissioned DLT platforms, suffer from performance and scalability issues. However, this is not to say that permissioned DLTs perform better to the level suitable for the volume transactions demanded by financial systems. Those who wish to deploy DLT, whether for Proof-of-Concept projects, pilot trials or actual commercial production, need to look beyond their immediate needs and assess carefully whether their DLT solution is scalable to their target and future performance requirements.

Resilience and business continuity are two major issues associated with the stability and systemic risk of using a particular technology. Although DLT is meant to be resilient by design, many factors relating to specific implementations and peripheral support, such as the resilience level of the communication network on which it runs, may affect its overall resilience. Sections 6.5 and 6.6 in Chapter 6 on Governance and Control discuss these issues in more details.

5.4 Technology and operational risks

Given that the deployment of DLT involves outsourcing or the use of technologies such as cloud technology, the relevant HKMA regulatory guidance may need to be followed. Such regulatory guidance, in the form of Supervisory Policy Manuals (SPMs) or supervisory circulars, includes, among others, Outsourcing (SA-2), General principles for technology risk management (TM-G-1), and Business continuity planning (TM-G-2). SPMs and circulars are available on the HKMA website[3], and these may be added to and updated from time to time due to technological advancements and industry developments. Those planning to deploy DLT, whether by themselves or through third party service providers, should recognise that supervisory guidance specific to DLT implementation may not necessarily be available because of the fact that DLT is still evolving.

Chapter 6 also identifies possible additional information and communications technology (ICT) controls to address potential technology risks arising from implementing DLT for financial applications. These ICT controls include security management, system development, information processing, and networks and communications.

5.5 Reporting and transparency

Reporting and transparency of financial data are important aspects of prudential regulation by overseers. In the past, it has often been the responsibility of financial institutions to prepare reports on a regular or ad hoc basis. The use of DLT opens up the possibility that regulators or auditors can directly access transactional data stored on the DLT ledger through a so-called “supervisory node” for monitoring or fraud detection and prevention, on a near real-time basis. Regulatory reporting and financial reporting (e.g. the filing of tax returns) can be made possible through the supervisory node. Those who are looking into deploying DLT should therefore consider the possibility that an independent party, such as a regulator or auditor, may request access to relevant transaction data. DLT design and related agreements may have to take this into consideration to ensure that allowing such access is permissible.

5.6 Governance and controls, cybersecurity and legal risks

Due to their substantive nature, the topics of governance and controls (also covering technology risks, cybersecurity and resilience) are separately discussed in Chapter 6, while legal issues are deliberated upon in Chapter 7.

5.7 Conclusion

Compliance issues for financial institutions or systems cover a wide range of concerns, including financial, operational, technological, personnel and legal matters. This chapter cannot cover them all, especially since some issues are specific to particular types of financial institution or applications. However, the chapter offers a solid starting point to help those engaged in DLT design and deployment be aware of the implications from the outset, avoiding the need for after-thoughts or “bolt-on” measures which are often costly and ineffective.

[3] SPMs may be found under http://www.hkma.gov.hk/eng/key-functions/banking-stability/supervisory-policy-manual.shtml.

Chapter 6

Governance and Control

6.1 Background

Chapter 7 of the first Whitepaper set out a number of potential governance and control issues which need to be adequately addressed prior to the implementation of DLT in financial applications. To address these issues, the HKMA has sought contributions from Deloitte Touche Tohmatsu and PricewaterhouseCoopers in relation to general governance and control principles. Details of their contributions are set out in Annexes D and E respectively. This chapter highlights some of the key principles suggested by these two firms, and adds input from the HKMA's Fintech Facilitation Office. The key general principles can be broadly categorised into the following five control areas:

- Governance
- Security Management
- System Development and Change Management
- Information Processing
- Communications Networks

As explained in Chapter 5, there is no specific regulatory guidance regarding the implementation of DLT. Reference can be made to the HKMA's Supervisory Policy Manuals on General principles for technology risk management and Business continuity planning and other relevant guidelines when applying the general principles set out in this chapter to the implementation of DLT in financial applications, bearing in mind that DLT is still evolving and not all risks associated with DLT may have been adequately identified and understood.

Given that access to financial applications is normally restricted to authorised users, and that such applications are expected to implement stringent governance structure and controls, it is likely that a permissioned DLT platform will be adopted in most cases of DLT implementation. Therefore, the discussion in this chapter only focuses on general governance and control principles for a permissioned DLT environment.

6.2 Governance

6.2.1 Governance structure

The distributed nature of DLT has the advantage of avoiding a centralised party who has absolute and full control of a platform. In an unpermissioned DLT platform, trust regarding the validity of a transaction is gained through a self-governing model that leverages DLT's built-in strong cryptography algorithm and consensus mechanism. However, in a permissioned DLT platform, appropriate legal arrangements and an effective governance structure are essential.

In general, there are many possible governance and operating models for permissioned DLT platforms. Below are several examples of feasible approaches and models:

- A consortium-like approach:- where several financial industry players join together to form an organisation with a governance committee, which manages the governance structure in order to achieve the common goals of the DLT platform;

- A joint venture approach:- where a separate autonomous entity is established by two or more financial institutions, through which the ownership, returns, and risk and governance responsibilities of the DLT platform are shared; and

- A statutory organisation approach:- where a statutory or regulatory body creates an organisation for governing and maintaining the operations of the DLT platform.

These three governance approaches and models have their own pros and cons in terms of cost, flexibility, time required for setup, legal certainty, market/industry recognition, and level of control. Institutions should consider their own circumstances before deciding on the most appropriate approach and model. A detailed analysis of these models is set out in Section 1 of Annex D.

Whichever governance approach or model is chosen, financial institutions should ensure that there is a proper definition of the Intellectual Property rights relating to the ownership of and access to the DLT applications and infrastructures. There should also be agreed dispute resolution mechanisms, covering issues such as how costs are shared and how liabilities are divided among the participants. All these should be cleared by a formal legal review. Also, the roles and responsibilities of members of the governance body should be formally agreed upon and documented. This should be done at the design and development stage, not after the launch of the DLT platform.

6.2.2 Membership on-boarding and ongoing operation

It is essential that a permissioned DLT environment has a set of commonly agreed on-boarding and operating rules to ensure that only authorised participants are allowed to access the platform, and that the platform is operated in an effective and efficient manner. A typical implementation of DLT for the financial industry would require the participants involved in any transaction to be traceable. Verifying the identities of the participants involved in any transaction usually relies on the Public Key Infrastructure (PKI) employed in the DLT environment.

On-boarding rules normally cover the following areas:

- **Due diligence:**- adequate due diligence should be performed for all new members to ensure that they meet applicable anti-money laundering requirements. The due diligence process can be performed by certain participants or by a designated party;

- **Security:-** as part of the on-boarding process, the governance body should ensure that the new member has implemented adequate cybersecurity measures and an effective internal control environment to prevent and detect any possible attacks on the DLT platform arising from its connection with the new member;

- **End-user agreement:**- prior to joining the platform, the new member should agree to and formally sign a legally binding end-user agreement making the member eligible to be connected with, obtain information from and conduct transactions on the network.

These governance and operating rules should apply to members not only for the on-boarding process, but also on an ongoing basis. The governance body should have an ongoing monitoring process and a re-certification mechanism in place to ensure that members continue to comply with these rules. Tiered membership is essential in any discussion of membership management in DLT. A typical DLT deployment usually has a clear distinction between nodes in terms of their roles and their access to privileged actions. For instance, only validating nodes can make a transaction committed, whereas common nodes are only able to propose new transactions. More restrictive rules may apply to some nodes, allowing them only to read transactions, or parts of them.

A very strong identity framework must be established to guarantee the identity of the participants involved in any given transactions. Transaction verification under a DLT environment relies heavily on PKI. This is because digital signing of transactions is an essential feature, as it provides trust in the system, guarantees non-repudiation of activities performed, ensures accountability and supports any possible claims process. Therefore, the processes related to key management for membership on-boarding and off-boarding, in terms of issuance, revocation and recovery, need to be carefully established. Although PKI can bring benefits in terms of providing encryption and generating trust, it also poses risks to a DLT system. One possible systemic risk associated with DLT is that PKI could be undermined if fraudsters are able to develop the computing ability to crack the keys.

6.2.3 Technology audit

A technology audit of a DLT platform is a challenging task, as DLT technology is still evolving and many new features continue to be developed. Also, a DLT platform usually uses smart contracts for automating certain processes, adding further complexity to the conducting of DLT platform audits.

Despite these technical challenges, the governance body should arrange for regular technology audits, such as audits of smart contracts, to ensure that proper governance and controls are in place. Smart contracts are pre-written executable programming codes/logics stored in the DLT platform. In some DLT platforms (e.g. Hyperledger), smart contracts are used to add records onto the chain. When performing a technology audit of the processes and controls associated with smart contracts, the following activities and processes should be reviewed:

- Approval of changes made to smart contracts;
- Administration of the access controls for smart contracts (e.g. who can deploy or activate a smart contract);
- Processes relating to the backup and recovery of keys, key protection and key revocation; and
- The use of oracles to verify the trustworthiness of the data sources (including external data sources), and the process or procedures for selecting these data sources.

6.3 Security management

6.3.1 Information protection

As in traditional application systems, access to read or update data on a DLT network is restricted to a 'need' basis, based on information/data classification that identifies which sets of data need to be protected. This information/data classification process, as well as the policies for approval, granting of access, and retention and destruction of information, should be properly established and documented.

In a typical permissioned DLT platform, only essential and non-sensitive data (e.g. hashes) are stored on-chain for efficiency and data privacy reasons. On-chain data, which is data copied to each node of a DLT network, is normally linked to off-chain data sources, which are large databases containing sensitive personal and transaction data that are either managed by centralised trusted parties or stored in a distributed file system. Information protection mechanisms should be in place for both on-chain and off-chain data.

Traditional information protection approaches, such as encryption and access controls, should be adopted for off-chain data so that only authorised parties can access sensitive data.

Besides these traditional controls, it is also important to keep the hashes of off-chain data in the DLT platform. The immutable nature of DLT can thus ensure that the integrity of the off-chain data is maintained. Regarding on-chain data, DLT platforms can, and most likely will, be connected to multiple external parties, making on-chain data available for participants in the DLT network. Therefore, proper data encryption should be required to ensure that access to data is restricted to authorised parties only.

6.3.2 Data privacy from a governance point of view

The shared and immutable nature of DLT allows many innovative designs and implementations of DLT for financial applications. However, it also creates potential issues relating to personal data privacy according to jurisdictional legal requirements on privacy, because personal data may be included and processed in a DLT platform. Therefore, adequate measures are required to ensure compliance with data privacy requirements.

Some DLT implementations may provide services and process information across more than one jurisdiction. It is therefore important to consult appropriately (e.g. by seeking legal advice) on whether privacy-related legal requirements have been catered for. Below is a list of some measures commonly adopted when personal data needs to be used, processed and stored on a DLT platform, but it is by no means exhaustive.

- Privacy impact assessment:- A privacy impact assessment is normally one of the first activities conducted to assess data privacy risks and address possible regulatory requirements when personal data is used, processed and stored on a platform. This assessment will provide further insights into the privacy issues relating to an envisioned DLT application, and will provide a useful point of reference that will help ensure compliance with privacy and data protection regulations. It is therefore desirable to conduct the assessment at an early stage of development so that relevant controls can be included at the design stage, thus minimising privacy compliance costs that may arise during the platform's operation.

- Tokenisation[1]:- Another possible approach to anonymise the data stored on a DLT platform is tokenisation. Each participant replaces the sensitive information it owns with a unique token and manages its own mapping between sensitive data elements and tokens.

- A Merkle tree is a common structure for safely redacting parts of the data of a transaction while ensuring the verifiability of the remaining data.

6.3.3 Authentication and access control (key management)

As discussed above, DLT leverages PKI to ensure strong security controls over transactions. User access to transactions and data, and users' ability to spend digital assets or initiate new transactions, are governed by a public and private key pair. Private keys are the direct means of authorising activities in a DLT platform. These keys are unique, and if lost, cannot be recovered in normal circumstances.

It is therefore important to ensure that security controls over private keys used for accessing the system and decrypting private data are in place. If private keys are accessed by an adversary, all wallets and assets secured by these keys will be compromised.

Against this background, stringent key management controls, including both physical and logical controls, are of the utmost importance. Robust key management is not only important for end-users (wallets in some DLT cases), but also for back-end administration. The controls could cover the following areas:

- Hardware security module[2] (HSM):- An HSM is a technology solution for safeguarding and managing digital keys. A successful DLT system needs highly reliable methods of interfacing with the strong key protection practices afforded by an HSM, especially for DLT administrators who need to maintain the public and private key pair.

[1] https://www.enterpriseinnovation.net/article/survey-says-fsis-need-encryption-and-tokenization-limit-exposure-cloud-539611032

[2] A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication, and which provides crypto processing.

Moving the cryptographic functions from software to dedicated hardware devices can provide better protection. HSMs can be clustered for greater performance and availability, allowing encryption functions to scale without sacrificing security. By relieving servers from performing processor-intensive calculations, an HSM also increases operational efficiency. To mount a successful attack, attackers either need to have administrative privileges, access to data before encryption, or physical access to the HSM. Some DLT platforms may only support one centralised certificate authority. That said, an HSM could be the single point of failure, so a redundancy set-up for HSMs needs to be in place;

- Recovery agents:-engagement of recovery agents as trusted third-parties who keep the keying materials required to recover keys should be considered as a possible option.

6.3.4 Security administration and monitoring

A distributed ledger node within a private DLT platform is still a combination of data and software running on one or more servers, most likely within a Virtual Private Network (VPN), and hence standard controls apply to the DLT platform.

As with traditional control environments, a security administration function and a set of formal procedures should be established. Such procedures should, among others, include virus checking schedules, the zero-day exploit remediation process, maintenance schedules, capacity and backup management, incident reporting, and escalation and response procedures.

Whereas traditional databases are controlled by a centralised administrator, a permissioned DLT platform is governed by a consensus mechanism. This in turn is administered by a central governance body, or an administrator appointed by the governance body. Either the governance body or the appointed administrator should be subject to proper control procedures and audit to detect and prevent unauthorised or fraudulent activities in a timely manner. Two suggested controls are given below.

- Staff engaged by the governance body, or the appointed administrator, should be subject to background checks; and

- Any activities involving privilege, power or special authority should be approved and monitored.

The decentralised nature of DLT platforms also calls for modifications to the current security administration model and protocols. The attack surface increases as the number of end points increases, making the risk of cyberattacks more likely. It is therefore essential that only authorised users and nodes can actually perform activities in the network. Also, the activities of external parties on the platform should be carefully controlled and monitored. Any nodes which have growing processing power or are executing a significantly high number of transactions should be carefully monitored, and concerns should be escalated to management for follow-up if necessary.

6.3.5 Physical security

The decentralised nature of DLT platforms warrants placing an additional focus on physical security, due to the presence of multiple nodes that provide a large number of physical access points. Traditional control environments and physical security measures, such as CCTV, physical barriers, physical key management and access controls should be implemented based on standard principles.

In addition, one approach for reducing unauthorised physical access is to centralise facilities, specifically by implementing a DLT platform within one or a few strictly controlled locations. This arrangement will reduce the number of physical access points to the DLT platform, but it may undermine the platform's resilience in case of power failure.

6.4 System development and change management

6.4.1 System development

A new system development element being introduced in DLT is the smart contract. In smart contracts, the programming codes/logics begin to execute when certain conditions are met, or specified dates are reached.

Smart contracts implemented on a DLT platform normally contain interfaces (e.g. for retrieving information from off-chain data sources), business rules, and data (to keep track of states of events). Interfaces, business rules and data need to be changed over the lifetime of the platform, because:

- Data that is used to keep track of states of events for triggering the contractual conditions will change once the pre-defined events occur;
- Business rules might change due to business decisions agreed upon by counterparties (for example, a counterparty may agree to a change in the settlement date in some cases); and
- The interfaces may change if there is an upgrade of the platform, say, for patching a security hole.

At some future date, data stored in one contract may need to be migrated to another contract, and the contract design should always ensure that such data migrations can occur in case the DLT platform needs to be upgraded.

Some smart contracts may also contain complex codes or logics which could easily have hidden bugs embedded within them. The Decentralised Autonomous Organisation (DAO) incident[3] is a famous one in which hackers exploited a vulnerability inside a DAO smart contract to drain more than 3.6m ether (the cryptocurrency on Ethereum) from the platform. Apart from intentional attacks, poorly written smart contracts can also disrupt a DLT system.

The suggested controls set out below can help prevent similar incidents from happening:

- Just as is done in the development of traditional applications, standard libraries and interfaces that have been thoroughly tested as building blocks of new smart contracts can be reused. This can help reduce the development time required, and minimise the chance of programming errors in the smart contracts;
- Code reviews should be performed according to industry best practices;
- A robust governance process should be put in place to ensure that changes to smart contracts are valid and agreed by all participants. The governance body should establish a control process for reviewing and signing off the deployment of a smart contract before it is activated;

[3] https://www.bloomberg.com/features/2017-the-ether-thief/

- The governance body should formulate a process that will identify and remove any malicious programmes from the network; and

- Agreed-upon standard interfaces (such as the ERC20 token standard for Ethereum) should be adopted to reduce the risk of security holes being introduced by non-standard interfaces.

Apart from controls related to smart contracts, traditional controls related to system development are still applicable, and attention should be paid to these also.

6.4.2 Portability and compatibility

The rapid evolution of DLT can lead to new versions of DLT platforms being released every few months, as there is a growing demand for new implementations and changes.

One commonly adopted industry practice to increase the portability and compatibility of application logics is to detach the application logics from the input/output code of the DLT layer. Increasing the portability of application logics on a DLT application could improve overall sustainability. This can be achieved by encapsulating the input/output codes by building abstracted application programming interfaces (APIs) to standardise the ways for reading from or writing to a DLT platform. Figure 1 illustrates how such portability can be achieved.

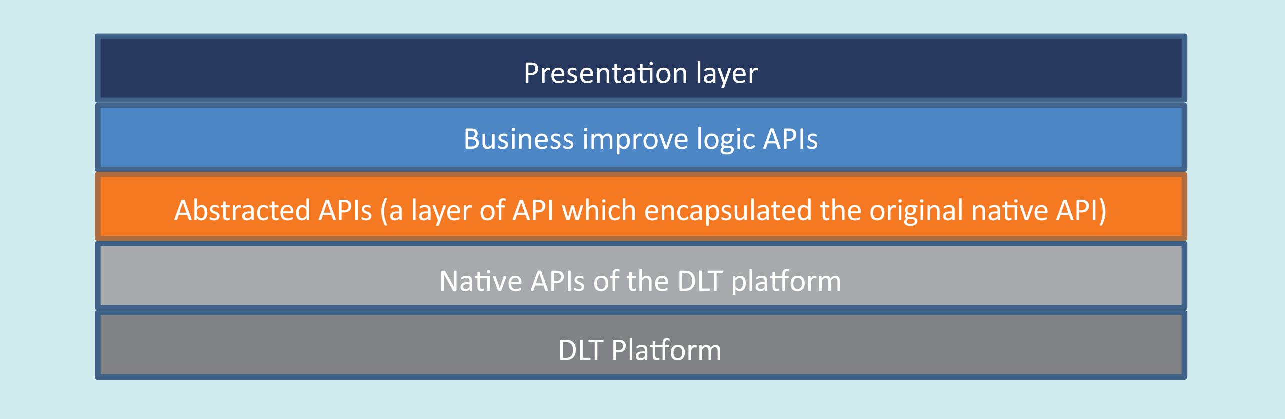

Presentation layer
Business improve logic APIs
Abstracted APIs (a layer of API which encapsulated the original native API)
Native APIs of the DLT platform
DLT Platform

Figure 1

The effectiveness of the abstracted APIs is demonstrated by our PoC trade finance application work, set out in Annex A. In this case, the trade finance application was originally built on top of the Ethereum version parity. It was then ported to the Hyperledger Fabric version 1.0 in less than half the original development time. This was done relatively quickly and smoothly because of the abstracted API layer between the DLT platform and the business logic, as shown in Figure 1 above. Such a design gets rid of the need to rebuild the whole application from scratch. Only the abstracted API layer, which mainly contains basic function calls to the DLT platform, needs to be re-built, and this requires limited effort.

Some advanced implementations may include subscription-based models or push mechanisms. In these cases, other implementation techniques can also be considered for use together with the abstracted APIs.

6.4.3 Change management

A DLT platform normally involves a number of participants. In some DLT designs, new developments or changes can be made and deployed from any node with access or connection to the network.

New developments and system changes to current functionalities need to be properly handled to avoid possible confusion to participants and unnecessary disruption to operations. A mechanism should therefore be in place to engage and seek consensus among all the participants prior to any new functions or changes being implemented on the DLT platform. Participants should also be given enough time to accept new developments or changes within a reasonable timeframe. It is also important to ensure that only authorised users are granted permission to accept new developments or changes.

The recent Bitcoin split[4] is a good example of such a change, and illustrates the importance of having proper change management and conflict resolution strategies to ensure that a unique outcome can be agreed upon within a reasonable time in a DLT environment.

6.5 Information processing

As the information processing and computer operation controls for centralised operating environments are also generally applicable to DLT operating environments, any DLT implementation should ensure that relevant and adequate controls are implemented for IT operations management support, performance monitoring and capacity planning, and IT facilities and equipment maintenance applicable to a centralised environment, in order to reduce the risk of operational disruptions.

One area in which DLT needs special attention due to its distributed operating environment is the design of disaster recovery and business continuity management processes. Some specific control principles which require special attention are set out below.

6.5.1 Disaster recovery and resilience

This heading can be categorised into two main topics:

- Network malfunction, resulting in a loss of connection to the DLT platform (this may be applicable to unconventional DLT designs); and

- Compromise of data integrity, which, in a normal situation, would result in the rolling back of any changes made within a specific time frame.

Losing connection to the network could impact the normal functionality of a DLT platform. This assumes a more severe outage than just the loss of a single node, as institutions would be expected to maintain multiple nodes in multiple locations to avoid any single point of failure. Besides, the mechanisms of recovering a node from data in the other nodes have to be defined clearly.

A network can be configured so that normal operation continues even if one of the peers is unavailable. To achieve this, it is important that major network functions, such as node authentication or access authorisation, are not centralised. DLT platforms usually have a high degree of resilience and this characteristic should be leveraged.

To ensure the continuity of key management services, the key management infrastructure should take the following into consideration in its design:

- The technical integrity of the key generation mechanisms (Certificate Authorities, Hardware Security Modules);

- The authorisation layer around the key generation mechanisms; and

- The redundancy requirements, such as no data loss or node authentication outage.

[4] http://money.cnn.com/2017/08/01/technology/business/bitcoin-cash-new-currency/index.html

These three components should be planned carefully so as to minimise the attack surface area and to effectively increase operational security and continuity. Separately, the ability to recover data by reconnecting to the existing network nodes depends on the key management processes. Hence, it is crucial to ensure that the keys used to authorise access to the DLT platform can be recovered or recreated.

All these processes need review and involvement by internal security teams and possibly validation from external security specialists to ensure that best practices are adhered to in setup, implementation and testing. More information with respect to business continuity management and disaster recovery processes can be found in Section 6 of Annex D.

6.5.2 Minimum viable number of validating nodes

A permissioned DLT platform may not always have every node in the network acting as a validating node due to performance or governance issues. Under some consensus mechanisms, a minimum number of available validating nodes needs to be defined. In the event that the number of available validating nodes is less than the required minimum number, the DLT platform is unable to handle any new transactions. Institutions adopting a permissioned DLT platform with this kind of consensus mechanism need to take this factor into consideration when designing the architecture and recovery management processes of a network.

Different DLT platforms have different definitions of consensus. For instance, some DLT platforms only need parties to be involved in a transaction to perform the validation. In such a situation, fault tolerance and resilience are not available in the design, and resilience may need to be built in at the infrastructure level rather than relying on built-in DLT resilience design. That said, the architecture design must be tailored based on the DLT platform selected to achieve the desired resilience level.

6.6 Communication networks

6.6.1 Security and network connectivity among nodes

In a normal DLT environment, each participating node in the network is allowed to connect with all other nodes within the same network. This is how a distributed and resilient environment can be maintained. However, this may create issues for some large-scale DLT platform implementations.

In a global network, thousands of direct participants (or even more) may establish a node. If certain participating institutions host their nodes locally inside their own network, such an arrangement may result in many external participants/nodes having a direct connection to those nodes. Many of these external nodes may need to go behind the institutions' firewall(s) to make the direct connection, which could open up undesirable connections from outside the network and increase the risk of cyberattacks. There are a number of possible ways to address this issue. In particular:

- As a DLT node is similar to a database which normally contains sensitive information, it is not desirable to locate the DLT node within a De-Militarised Zone (DMZ). A possible option is to set up a gateway in the DMZ which can redirect authenticated requests to the DLT node residing in a more secure environment, subject to the availability of a gateway solution;

- Apart from putting the node on-premises, it may also be feasible to set up all the nodes of the DLT platform in a common infrastructure. This common infrastructure can provide a hybrid cloud service to all participating institutions. As a result, institutions are only required to connect to one service provider in a secure manner;

- A hybrid of the above two options:- an institution may only communicate with a limited number of nodes (say, only to local participating institution nodes), and a common gateway set up with high availability can be leveraged to connect with nodes outside the local community.

6.7 Outsourcing

The development and operation of a DLT platform may involve cooperation with third-party service providers, so the risks related to outsourcing should be considered carefully. When financial institutions assess risks related to outsourcing, they tend to focus on aspects of due diligence, such as the financial condition, technical capability, and oversight and monitoring activities of the service providers. This means they can sometimes overlook the impact that having a small number of service providers can have on risk.

The entry barriers to the service provider industry, including infrastructure requirements and technical capabilities, are relatively high. As a result, many financial institutions rely on the same provider. This increases concentration risk which, together with institutions' growing reliance on fintech services, means that technical or operational issues affecting certain fintech providers could pose systemic risks to financial institutions within and across borders, and even create risks for the entire financial system.

Financial institutions should work together with their service providers to prepare contingency/recovery plans for worst-case scenarios. Service providers could also consider segregating their infrastructures and/or services by geography, industry or financial services segment in order to mitigate systemic risks.

6.8 Other considerations

When considering the controls required for DLT implementation during the development process, certain standard controls such as those present in ISO 27001[5], the Center for Internet Security Controls[6] and SANS Critical Security Controls[7] should also be taken into account. Relevant controls should be adequately implemented as part of a comprehensive cybersecurity control programme, with regular reviews and audits conducted to ensure compliance.

Since cryptographic algorithms are widely used in typical DLT implementations, it is important to have some clear control principles in place for selecting the right algorithms. In general, standardised algorithms that have been publicly scrutinised are preferable. In addition, the security of these algorithms needs to be regularly reviewed, since new vulnerabilities (in design or implementation) even of standardised algorithms are not uncommon. For instance, trapdoors have been found in the elliptic curve secp256r1, which is widely used in digital signature schemes.

Advances in technology may also impact DLT reliability. For example, emerging technologies such as quantum computing may pose a security risk to DLT. While not an immediate threat, quantum computing has the potential to threaten the security of asymmetric cryptography, an essential element of DLT.

[5] https://www.iso.org/isoiec-27001-information-security.html

[6] https://www.cisecurity.org/controls/

[7] https://www.sans.org/critical-security-controls

6.9 Conclusion

This chapter highlights a number of key control principles governing possible financial applications using DLT. These key principles include governance, security management, information processing, and business continuity. The suggested key principles are not meant to be exhaustive, and institutions should also take into account their own implementation experience and any in-house control requirements when applying DLT to their own application development. In addition, given the rapid developments in DLT and the fact that new releases and versions of DLT are regularly introduced to address new issues, readers should not confine themselves to the suggested key principles in this chapter during DLT implementation, but also include any new control concepts and requirements as they evolve. Finally, the following two control areas require more attention, study and consideration going forward.

First, authentication and access control (key management) under security management is an area requiring very stringent controls in addition to conventional ones. This is due to the adoption of the advanced and complex technology of cryptographic algorithms, which play a critical role specifically for systems built on DLT. Without sufficient controls, a hacker will have a better chance of gaining access to private keys, and digital assets secured by these keys could be compromised. Similarly, if sufficient controls are not in place, digital assets may become permanently irrecoverable in the event of the loss of a participant's private key. Therefore, controls such as the use of HSMs, multiple signatures and key revocation and recovery agents are essential. Further study is recommended to identify additional controls for ensuring the safety and soundness of DLT platforms.

Second, smart contracts represent another complex area requiring further study. The new protocol of the consensus mechanism is also creating brand new challenges, as there are not many precedent use cases that can be referred to. The DAO incident previously mentioned is a good reminder of the disastrous consequences of a lack of sufficient code review.

Undeniably, while advanced technology can bring many benefits to an industry, it can also create new challenges. We would like once again to stress that this chapter only provides key control principles that are relevant to the implementation of DLT solutions, and is by no means exhaustive. It is imperative to have a strong governance model under which all stakeholders can regularly review and stay abreast of the latest developments in the technology.

Chapter 7

Legal Issues

7.1 Background

Chapter 10 of the first Whitepaper identified a number of potential legal issues arising from the use of DLT. This chapter provides a more in-depth discussion of those issues. They may be broadly divided into the following areas:

1. Legal basis
2. Data protection and privacy
3. Cross-border and localisation issues
4. Smart contracts
5. Liability
6. Competition/Anti-trust laws
7. Legal issues in specific applications

The HKMA is honoured to have received professional contributions from The Law Society of Hong Kong and academic input from law professors Dirk Zetzsche, Ross Buckley and Douglas Arner in response to these potential legal issues. Details of these contributions are set out in Annexes F and G respectively. This chapter summarises these contributions and suggests some ways of addressing the issues. However, this chapter and the detailed analyses in Annexes F and G only provide some preliminary observations and suggest some general principles relating to the potential legal issues, and should not be considered as legal advice. Additionally, DLT continues to evolve rapidly and new technological concepts and models are constantly being built or derived from DLT. Anyone considering adopting a specific application of DLT should seek legal advice to ensure that all possible legal issues are adequately addressed.

This chapter focuses only on the use of permissioned DLT platforms for financial services. Although the following discussion concentrates on the Hong Kong context, it also takes into account the legal requirements of some overseas jurisdictions due to the growing adoption of DLT for some cross-border initiatives. Many of these general principles are also applicable to other jurisdictions.

7.2 Legal basis

DLT is good at replacing processes that are labour intensive or involve a lot of paperwork, as it helps to manage and track the movements and execution of digitised documents. Generally the validity and enforceability of digitised documents depend on mutual agreement between participating parties, so such uses should be adequately addressed in the contracts or terms and conditions of any DLT solutions. Furthermore, if a DLT solution wishes to use digital signatures to authenticate legal documents, checks should be carried out to ascertain whether digital signatures are recognised under local legislation. For example, the Hong Kong Electronic Transactions Ordinance (ETO) gives the same rights to digital signatures as to handwritten ones for legal documents for government use, and allows private parties to agree on the same. However, checks should also be done on any exclusions, such as the exclusion under the ETO of the use of digital signatures for any assignment, mortgage or legal charge within the meaning of the Conveyancing and Property Ordinance.

More detailed discussion on the legal basis of deploying DLT may be found in Sections 11, 12, 13 and 15 of Annex F.

7.3 Data protection and privacy

In some cases, personal data will be stored in the ledger. In Hong Kong, the handling of personal data is regulated under the Personal Data (Privacy) Ordinance (PDPO), so the six data protection principles (DPP) under the PDPO, including the definition of personal data[1], apply. However, as the PDPO is based on the privacy principles of

[1] The first part of this leaflet gives a basic introduction: https://www.pcpd.org.hk/english/resources_centre/publications/files/PCPDbooklet_about_the_PCPD_201509.pdf

the Organisation for Economic Co-operation and Development (OECD), the following analysis also applies to jurisdictions that have data protection laws based on the OECD privacy principles.

Of the six DPPs, DPPs 1 and 3 state that personal data is to be collected and used for a direct purpose of the data user, while DPP 2 provides that personal data is to be kept accurately, and no longer than necessary.

The three key characteristics of DLT that need addressing under the PDPO are, first, the accessibility of some DLT platforms, in which all nodes have equal access to all stored personal data regardless of whether they need to see it; second, the immutability of stored data, whereby data cannot be amended or erased; and third, the often cross-border nature of DLT, meaning that personal data may be stored outside Hong Kong.

If personal data can be accessed by all nodes of a DLT platform, DPPs 1 and 3 may be contravened unless there is some justification for all nodes to have such access. It is worth noting, however, that some versions of DLT can be configured so that not all stored data is replicated to all other nodes. Even so, such a version of DLT faces the second challenge of immutability.

To address the DPP 2 requirement for accurate data, it may be acceptable to maintain the accuracy of data by superseding older data with newer data, and having a system in place to ensure that only the most up-to-date data is used. However, such an arrangement still does not resolve the issue of the retention requirement under DPP 2. Even though the PDPO does not give individuals the right-to-be-forgotten or the right-to-erasure, it does require that any personal data that is no longer needed by a data user should be deleted.

One development noted is a DLT design that allows the redaction of stored data. Inevitably such a design weakens the very foundation of DLT — its ability to guarantee the integrity of non-repudiated data — so its use may raise more questions than it answers. Organisations considering such a kind of redactable DLT deployment will need to weigh up the benefits carefully.

Against this background, the simplest way to address privacy concerns would seem to be to avoid storing personal data in the ledger, but rather only keep the hashes of personal data in it. Storing personal data off the ledger in more conventional databases while keeping hashes in the ledger could continue to ensure data integrity while controlling and limiting access to personal data.

To address the immutability issue, it has been suggested that when encrypted personal data in a ledger is no longer needed, the corresponding encryption key could simply be discarded. This notion is fraught with problems, as such an arrangement would require almost every piece of personal data to have its own encryption key. It is also uncertain whether discarded keys could be regenerated or kept beyond their expiry. Furthermore, the increasing power and speed of computers makes it possible that encrypted data may be able to be decrypted in the future.

As a final word on the topic of the collection of personal data, data users should observe the PDPO regardless of whether data is to be stored using DLT or not. The Office of the Privacy Commissioner for Personal Data has published many useful guidance notes for data users on compliance matters. Among them is the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement[2], which may be useful in helping data users explain to data subjects how they intend to process the personal data that they collect.

More detailed discussion on data protection issues in deploying DLT may be found in Sections 1, 3, 4, 5 and 6 of Annex F.

[2] See https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf

7.4 Cross-border and localisation issues

The requirement under Section 33 of the PDPO that prohibits the transfer of personal data outside of Hong Kong unless certain conditions are met is not currently in force. If and when this becomes effective, the storage of personal data using DLT will have to be supported by conditions such as the consent of data subjects, the location of the storage being endorsed by the Privacy Commissioner, an assessment that the location of the storage operates under a substantially similar law as the PDPO, or other conditions as listed under Section 33 of the PDPO.

Other jurisdictions may have localisation regulations or legislation in place by which certain data stored in DLT, whether or not it is personal data, must remain in the jurisdiction or have a copy stored in the jurisdiction. In such cases, the purpose is often to ensure that law enforcement authorities of that jurisdiction can access the data. In a DLT platform, if the ledger is replicated to all nodes, then personal data belonging to one jurisdiction may be stored in another jurisdiction and therefore become subject to access by law enforcement authorities of that jurisdiction. Such an arrangement may be in conflict with the data protection regime of the first jurisdiction, and needs to be addressed.

These scenarios further reinforce the benefits of not storing personal data in the ledger, but only storing its hashes there for the purpose of integrity checks.

Other than these considerations relating to personal data, the cross-border nature of DLT also requires participants to consider their legal footing in terms of applicable law (i.e. which jurisdiction's law applies to the arrangement), applicable jurisdiction (i.e. which jurisdiction's courts resolve any legal dispute), and dispute resolution (i.e. whether arbitration is acceptable as an alternative to adjudication). There are no right or wrong answers to such questions, but it is vital that participants take the time to consider these arrangements and seek appropriate legal advice on common grounds that are acceptable to all. This suggests that at least a set of formal terms and conditions, if not a legal contract, should be drawn up to protect the interests of all participants.

More detailed discussion on the cross-border legality of deploying DLT may be found in Sections 2, 8 and 10 of Annex F.

7.5 Smart contracts

A smart contract may be considered as an arrangement whereby autonomous software running on a DLT platform automatically exchanges assets that are stored or represented on the DLT platform (e.g. the delivery vs payment arrangement). The autonomous nature of the software removes intermediaries and therefore reduces risk, while also saving time and money.

Whether a smart contract can be considered as a legal contract is still an open debate. However, the notion that smart contracts can be used to completely replace legal contracts or govern the relationships between participants in a DLT platform is misguided. Using a smart contract without explicit contractual terms could cause uncertainty for participants in the event of unforeseen consequences or disputes.

The Decentralised Autonomous Organisation hack[3] was a wake-up call and a reminder that programming/modelling errors and complex contract interdependencies can give rise to the risk of smart contracts failing to reflect the intention of the creator. Steps must therefore be taken to ensure that, if an undesirable consequence should occur, there is already a pre-agreed governance structure and contractual framework in place to handle the situation. Furthermore, the smart contract should contain an "escape hatch" enabling contracts to be modified or undone in the light of unforeseen eventualities.

The liability issue of smart contracts is covered in the next section.

[3] See one explanation at http://www.kwm.com/en/knowledge/insights/smart-contracts-open-source-model-dna-digital-analogue-human-20160630

More detailed discussion on the legal issues relating to smart contracts may be found in Sections 16, 17 and 18 of Annex F.

7.6 Liability

The issue of liability associated with participation in a DLT platform, including the use of smart contracts, is a complex one.

First of all, liability arising from harm or losses caused by a failure in the use of DLT (such as data breaches, hacking and non-delivery of assets) can be dealt with or be governed by the terms and conditions of contracts. In cases where there is no contractual relationship, liability is covered by the duty of care or tort, as in the case of negligence. As such, it is important that participants in a DLT platform fully understand the legal obligations that contractual terms and conditions impose on them. At the same time it is worth noting that the enactment of the Contracts (Rights of Third Parties) Ordinance in Hong Kong means that rights to third parties may be conferred, so any contractual terms will need to be carefully drafted to avoid unintended liability.

More detailed discussion on the direct liability associated with DLT may be found in Sections 7 and 9 of Annex F.

Furthermore, the notion that no one is in control and therefore no one can be held legally liable in an autonomous or disintermediated system such as a DLT platform or smart contract is unwarranted. It has been long established that owners of machines are responsible for the actions of the machine, so ownership or control over a DLT ledger can be a determining factor in the degree of liability vested to participants. Given the participative and decentralised nature of DLT, whereby control or even ownership of the ledger is shared, joint liability could be a likely outcome. As such, a party to the ledger, regardless of whether that party designs it, operates it, takes on administrative roles such as validator/ notary, or uses it in the simplest sense, may well share some liability. Therefore, before deciding to take part in a distributed ledger as a joint venture or multiparty contract, legal advice should be sought to understand liability. Participants should also consider factoring in an appropriate amount of risk capital or taking out insurance coverage.

More detailed discussion on the liability implications of DLT may be found in Annex G.

7.7 Competition/Anti-trust

DLT may pose a risk to fair competition if it functions as an artificial or technological barrier that enables or facilitates monopolies, for example by making it difficult for new members to join a ledger or to interoperate with an existing ledger and thus driving some firms out of the market. In such cases additional liability may arise from the relevant-competition/anti-trust law.

Given that competition law is relatively new in Hong Kong, the anti-competition aspect of deploying DLT may need to be carefully studied.

More detailed discussion on the competition law-related aspect of DLT may be found in Section III. D. 4 of Annex G.

7.8 Specific applications

Physical asset management

One of the most appealing uses of DLT is to tokenise physical assets so that smart contracts can be deployed to manage asset transactions. All parties in such arrangements are normally subject to private agreements and terms and conditions of use. The custodian naturally has a great responsibility to ensure that the physical asset is only released to the rightful owner, and therefore should develop sufficient proactive and reactive measures to facilitate a safe redemption process. Furthermore, all the legal issues highlighted in the earlier part of this chapter regarding liability and smart contracts also apply here.

More detailed discussion on the legal issues surrounding the use of DLT for tokenised physical assets may be found in Section 14 of Annex F.

Mortgages/e-Conveyancing

Procedures for the conveyancing of land are highly formalised and operate according to various statutory requirements. They often hinge on the key requirement that land transactions must be made in writing to be valid. In this respect, there is some uncertainty about whether Hong Kong law recognises computer-generated contracts as “writing”. Furthermore, the ETO was explicitly drafted to exclude electronic records as examples of “writing” and electronic signatures as “signing” for contracts for the sale of land and deeds for the deposition of land. It is therefore clear that, unless there is a change in government policy and legislation, electronic conveyancing is not a possibility in Hong Kong at the moment.

More detailed discussion on the issues that need to be addressed for electronic conveyancing to take place may be found in Section 19 of Annex F.

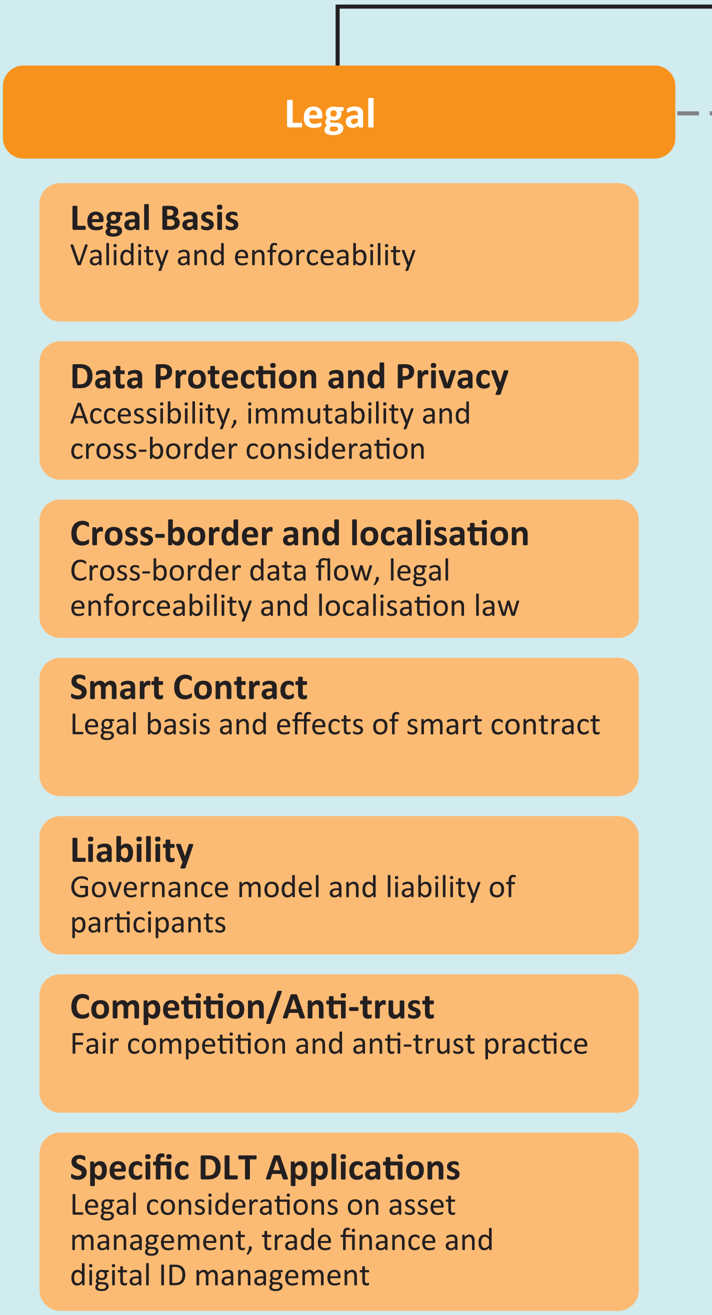
Trade finance

The use of DLT for trade finance can increase transparency of information along the trade chain, but such transparency of information belonging to multiple parties may need legal support. Furthermore, the legality of digitising many types of trade finance-related documents may also need to be studied.

More detailed discussion on the legal basis of digitising the workflow of trade finance may be found in Sections 20 and 21 of Annex F.

Digital ID Management

Using DLT for digital identity management inevitably touches upon the issue of privacy protection, and the PDPO should be studied carefully to ensure compliance. Furthermore, if the digital identity



Legal

Legal Basis
Validity and enforceability

Data Protection and Privacy
Accessibility, immutability and cross-border consideration

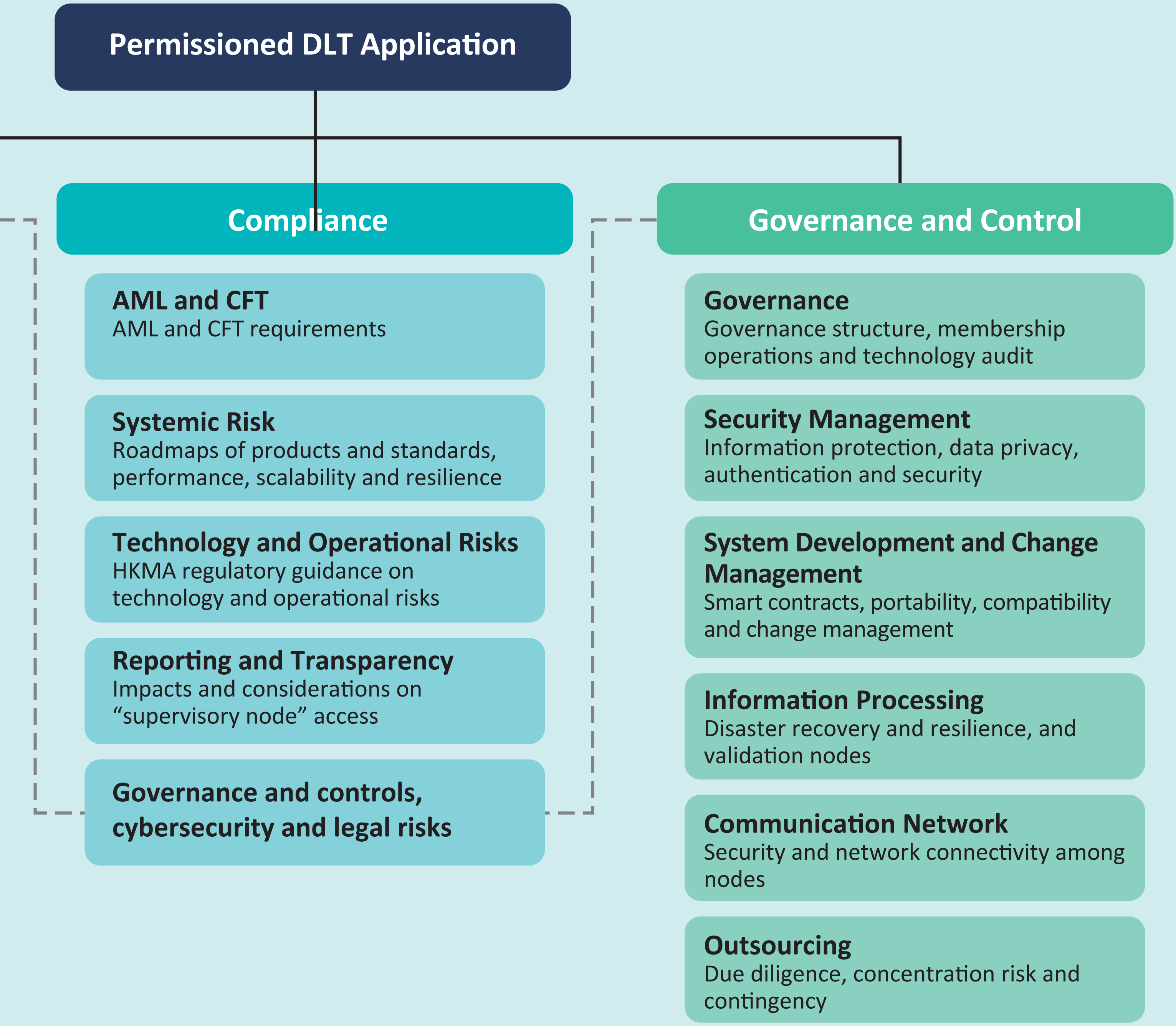
Cross-border and localisation
Cross-border data flow, legal enforceability and localisation law

Smart Contract
Legal basis and effects of smart contract

Liability
Governance model and liability of participants

Competition/Anti-trust
Fair competition and anti-trust practice

Specific DLT Applications
Legal considerations on asset management, trade finance and digital ID management



Permissioned DLT Application

Compliance

AML and CFT
AML and CFT requirements

Systemic Risk
Roadmaps of products and standards, performance, scalability and resilience

Technology and Operational Risks
HKMA regulatory guidance on technology and operational risks

Reporting and Transparency
Impacts and considerations on "supervisory node" access

Governance and controls, cybersecurity and legal risks

Governance and Control

Governance
Governance structure, membership operations and technology audit

Security Management
Information protection, data privacy, authentication and security

System Development and Change Management
Smart contracts, portability, compatibility and change management

Information Processing
Disaster recovery and resilience, and validation nodes

Communication Network
Security and network connectivity among nodes

Outsourcing
Due diligence, concentration risk and contingency

management application involves the collection of Hong Kong Identity Card images or numbers, the Code of Practice on the Identity Card Number and Other Personal Identifiers issued by the Privacy Commission for Personal Data should be consulted.

More detailed discussion on the privacy issues related to identity management may be found in Sections 22 and 23 of Annex F.

7.9 Conclusion

A number of legal issues, including legal basis, data protection, cross-border and localisation issues, smart contracts, liability, competition/anti-trust laws and legal issues in specific applications, have been discussed in this chapter.

The issue of legal basis is a fundamental one that needs to be addressed quite early in any project planning. While legal solutions are readily available, detailed analysis of specific DLT applications does need to be carried out in order to identify all possible legal basis challenges. As for the issue of data protection, there is no doubt that this poses one of the more challenging legal problems due to the impact of new technology and its escalating capabilities. One point worth noting in terms of future planning is that the EU's General Data Protection Regulation (GDPR), due to come into force on 25 May 2018, is expected to bring regulations into line with recent technological developments. However, its clarity, effectiveness and impact on the use of DLT for storing information related to individuals have yet to be tested. In the meantime, many data protection laws are being examined to see if they come up to the same standards as the GDPR. Those looking to implement DLT with personal data should therefore consider ensuring that their design is GDPR-ready.

Issues related to smart contracts, liability, and competition are also complicated because these issues are relatively new to the technology or to Hong Kong. As more DLT Proofs-of-Concept and DLT applications are examined and studied, the industry as a whole should accumulate more practical knowledge about these issues, and develop ways of handling them.

This chapter is not meant to provide an exhaustive list of legal issues and solutions. Rather, it offers a general appraisal of the types of legal issues that may be encountered when deploying DLT, so that users may be sensitive to them and seek legal advice at the appropriate time. More specific DLT applications will no doubt give rise to domain-based legal issues that will need to be dealt with in the future. Engagement with the legal profession is therefore encouraged as early as possible in any DLT-related project, so that its design takes all possible legal implications into consideration.

Chapter 8

Proof-of-Concept Work

8.1 Background

In the first phase of this research project on Distributed Ledger Technology, three use cases were selected for Proof-of-Concept (PoC) work: trade finance, digital identity management, and mortgage loan applications. All three areas share the fact that their underlying business processes involve multiple parties, are usually non-standardised, and are manually intensive, paper-based, and error-prone.

This chapter provides a summary of developments in the three PoC cases. It discusses the design decisions made, the benefits discovered and challenges encountered, and finishes with discussion of some considerations arising from the research. We would like to thank Deloitte, ASTRI and all the participating parties from the working groups for providing the technical assistance and business analysis to enable the development of prototypes within a short period of time. Detailed reports on each case are set out in Annexes A (trade finance), B (digital identity management), and C (mortgage applications) for readers looking for a more in-depth understanding.

8.2 General observations and lessons learned

8.2.1 Trade finance

The Prototype

The trade finance DLT use case covered trade finance arrangements on open account terms. The goal was to leverage the data distribution nature of DLT to achieve the following goals:

- To share the status of each transaction throughout the process with all trade participants in the ecosystem in order to prove the authenticity of all trade documents (e.g. POs, bills of lading and invoices);
- To create alerts on duplicated financing to reduce fraud loss;
- To automate selected manual processes with smart contracts and reduce the human effort required for invoice reconciliations; and
- To protect customer privacy and sensitive business information from other players in the network, and allow only authorised access to privileged data.

While the entire trade finance DLT prototype was hosted on cloud infrastructure, it was built in two layers, the data layer and the business application layer. The underlying data layer, which distributes data across the platform and facilitates consensus, adopts an open source DLT network such as Ethereum or Hyperledger. These networks have their own Application Programming Interface (‘API’) for system integration. On top of the data layer is the user interface and business application layer. However, large banks and corporates can integrate their own trade finance and trade systems with the underlying data layer without needing to use this application layer. Figure 1 in Annex A provides a detailed explanation.

Smart contracts have been used in a number of areas. One is to store the status of a transaction with a stated data structure so that enquiries can be made quickly. Another is to distribute event-triggered logic among nodes so that finance can be provided to customers more promptly based on “triggering events” built into the smart contract. Also, reconciliations between POs and invoices are automated in the DLT network using smart contracts.

Benefits and challenges

The benefits identified from the PoC work are summarised in the table below:

Benefit	Description
Transparency and Fraud-resistance	Increases transparency and lowers risk of fraud, helping to create trust among transaction parties
Error-resistance	Increases automation to lower error-proneness
Data access	Provides faster access to the data stored on the network
Efficiency and Cost-reduction	Delivers higher efficiency and lowers costs due to standardisation and digitisation of documents, and elimination of intermediaries and a central authority
Regulatory oversight	Offers real-time oversight and an immutable document trail

The challenges identified are set out in the table below:

Challenge	Description
Governance model	Requires a governance mechanism to be established
Data security	Requires cyber resilience of the platform and network recovery to protect distributed data
Industry Standards	Industry standards in areas such as data structure not fully established, though these are necessary for cross-border collaboration
Interoperability	Requires alignment and mechanism to enable the communication and interoperability between different DLT systems, between DLT systems and existing systems

Considerations

The next step is to move the PoC work on to the commercial pilot stage. Technology appears not to be the major obstacle, but issues regarding the governance structure, system integration, data storage and standards, and legal and compliance matters all need to be addressed before the project can move into production.

Governance Structure

Given that trade finance platforms normally involve financial transactions and sensitive banking data, a permissioned DLT platform is recommended. A governance mechanism and structure governing on-boarding, daily operations and monitoring, and dispute resolution is necessary to ensure that proper controls and security measures are in place. Three governance structure options were considered: (i) a “Working Group”; (ii) a “Private Sector Entity”; and (iii) a “Hybrid Entity”.

A “Working Group” would allow decisions to be made through information sharing as an association, but not as a legal entity by definition. Each participant would own and operate its own node, and contribute resources to drive common objectives forward. A separate, autonomous “Private Sector Entity” would own and develop the platform with the founding participants as core stakeholders. The platform would be offered as a utility to other participants who would operate their individual nodes. The third option, a "Hybrid Entity", is one where a public sector player would take on the governance role while private sector participants would sponsor the development and operation of the platform. The detailed implications of these governance structures are discussed in Section 6.2.1.

Data storage and standards

There has been some debate on what data should be kept "on-chain" and "off-chain". Storing all information on-chain would certainly maximise the value of the DLT network. However, it would also increase the risk of having a negative impact on network performance and difficulties in reaching consensus over a common data standard among participants. In general, data containing personal information is better stored off-chain. Further discussion on this subject can be found in Section 6.3.1 (Information protection) and Section 7.3 (Data protection and privacy).

Another debate centres around whether the stored data should be accessible by all participants or only by selected participants. As smart contracts are also distributed across the network, the intellectual property ownership of the smart contract software brings further discussion of the topic. The immutability of the ledger also gives rise to issues relating to data retention and housekeeping requirements.

Legal and compliance issues

Although Hong Kong has a legal framework that supports the application of DLT, disputes arising from cross-border transactions may involve international trade laws. A legal framework should therefore be established, preferably by a legal and regulatory committee that is able to represent Hong Kong in negotiations with other jurisdictions.

8.2.2 Digital identity management

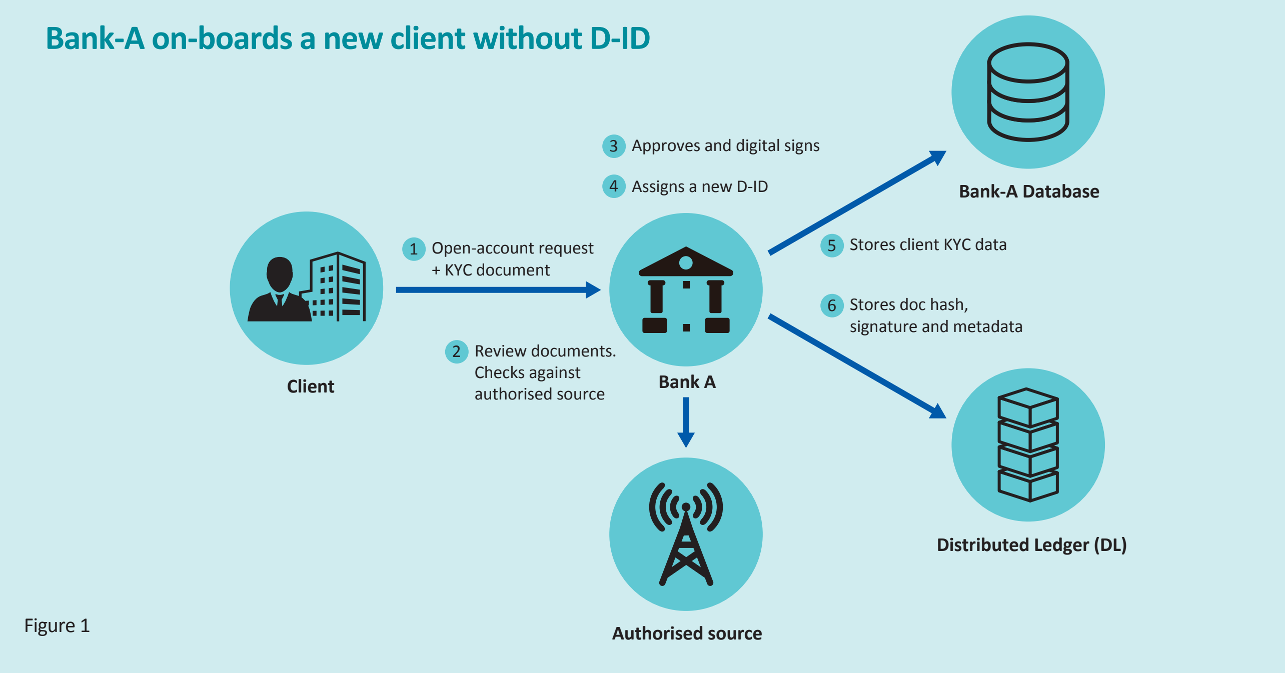
The Prototype

The second use case explores the feasibility of using DLT for digital identity management. Financial institutions are required to carry out the Know-Your-Customer (KYC) process as part of their customer on-boarding process, before they conduct business with a new customer. Customers are normally required to present their identification documents and have a face-to-face interview as part of this identification and verification process. There is thus an incentive for financial institutions to find a cost-effective and user-friendly solution for carrying out the KYC process. Digital identity management has been identified as a possible way of streamlining the KYC process, allowing multiple institutions to rely on the same source of digitised customer information.

In the first phase of this research project, a working group was formed to identify major issues and possible solutions and to ascertain whether or not DLT could provide an appropriate solution. In this second phase, the working group has formulated the following features and overall structure for the PoC prototype:

- selective customer information is stored as data on the DLT platform, which is immutable and auditable;
- the data stored on the DLT platform is verifiable through a consensus process;
- the data is simultaneously synchronised and maintained in multiple locations to provide data redundancy; and
- user privacy is protected transparently through a customer-controlled interface relating to banks' access to customer data.

In the prototype, if a customer does not possess a digital identity, one will be created for the customer. A relationship is then established between the customer and the participating bank (Figure 1). The bank will verify all the customer's important identity information, including digital documents, on top of the regular on-boarding KYC process, and store the hashes of the data and related metadata in the DLT platform, accessible by all other participating banks.

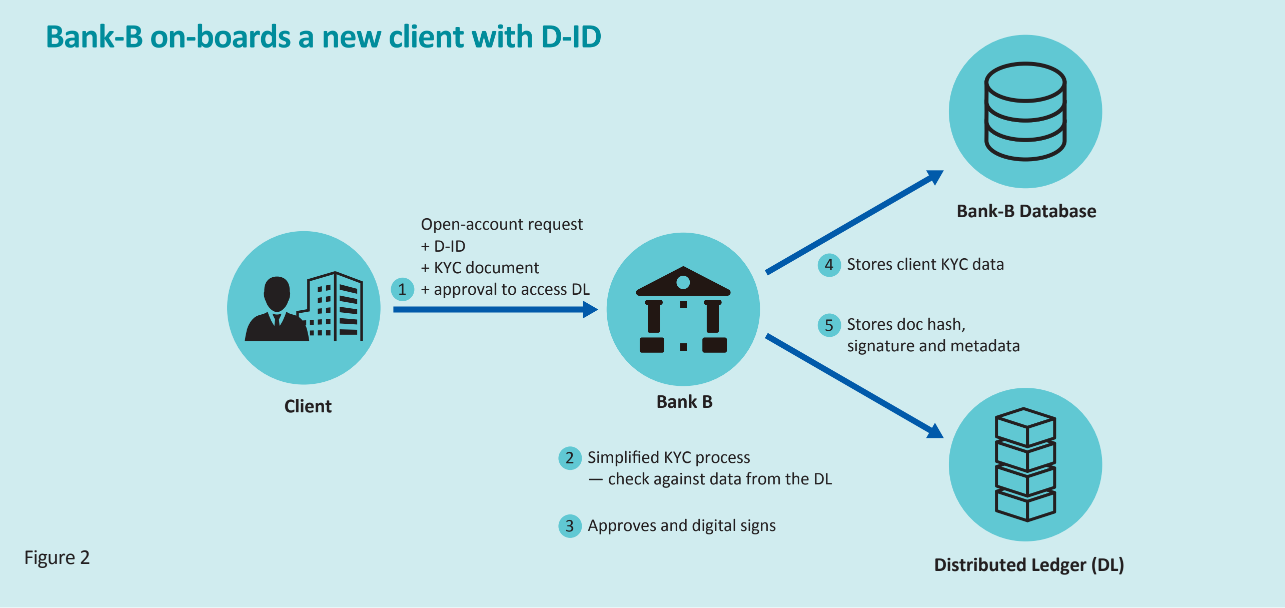


Bank-A on-boards a new client without D-ID

Client
1 Open-account request + KYC document
2 Review documents. Checks against authorised source
3 Approves and digital signs
4 Assigns a new D-ID
Bank A
Authorised source
5 Stores client KYC data
Bank-A Database
6 Stores doc hash, signature and metadata
Distributed Ledger (DL)

Figure 1

If the customer later establishes a relationship with another participating bank, that bank may utilise data stored in the DLT platform by comparing the hashes stored in the documents submitted by the customer for authentication (Figure 2).



Bank-B on-boards a new client with D-ID

Client
1 Open-account request + D-ID + KYC document + approval to access DL
Bank B
2 Simplified KYC process — check against data from the DL
3 Approves and digital signs
4 Stores client KYC data
Bank-B Database
5 Stores doc hash, signature and metadata
Distributed Ledger (DL)

Figure 2

An API enables the customer to check and update the stored data via a mobile application, and control the banks' access to the customer's data. Furthermore, the customer can apply for products or services provided by any of the participating banks (e.g. credit cards, account opening) through the mobile application.

Benefits and challenges

The benefits identified from the PoC work are summarised in the table below:

Benefit	Description
Sharing of previous KYC work by other banks	The work of verifying customer identity is shared among banks, thus cutting down on repetition and reducing overall costs
Improved Customer Experience	End-customers can control banks' access to their personal identification information, and apply for new products and services at any participating bank

The challenges identified are set out in the table below:

Challenge	Description
Legal and Regulatory Requirements	More work needs to be done to ensure customer privacy is protected, and relevant arrangements satisfactorily comply with legal requirements
Cyber security	The DLT platform must ensure that malicious validating nodes can be identified and excluded, and that cyberattacks will not result in network damage and data loss

Considerations

Sector-wide Platform vs Global Internal Platform

There are two configuration options for a DLT-based digital identity management system. The first one allows multiple banks to form a consortium with a high degree of collaboration among parties, or to jointly subscribe to the same digital identity service provider. The second one allows a global bank to use the platform across different jurisdictions and lines of business to consolidate its KYC work across them.

Given that multiple banks are involved in the working group, it was decided that the first option should form the basis of this prototype.

Data Stored

Discussion took place over what data should be stored on the DLT platform. To minimise the effort required to integrate this DLT platform with banks' internal KYC systems, the working group decided that the DLT platform should only store the hashes of the digital documents submitted by the customer, rather than the digital documents themselves. The original documents submitted by the customer should continue to be stored in banks' private databases, but additional supporting information can be obtained from the DLT platform to facilitate the banks' KYC work.

Choice of DLT network

As with the trade finance PoC work, the choice of DLT network was also an important decision requiring careful assessment. Whether the system is interoperable in a way that supports joint operations by multiple banks is something that will greatly affect whether or not banks will decide to join the platform. It will also affect the subsequent success of the platform, which will depend on how much of the banks' KYC work can be readily "shared" on the platform.

8.2.3 Mortgage loan application

The Prototype

As discussed in Chapter 11 of the first Whitepaper, the current mortgage loan application process is time-consuming, laborious, manually intensive and paper-based. This makes it an ideal area for which to explore the potential of applying DLT.

In the first stage of the research project, the working group for mortgage loan applications had arrived at the final stage of building the prototype for property valuation in the mortgage loan application process. In this second stage, the prototype has been completed. One of the banks participating in the working group further launched its commercialisation project to turn the PoC prototype into a fully functional commercial platform. Up to mid-October 2017, more than 15,000 property valuation cases had taken place on the commercial platform. The following sections discuss lessons taken from both the prototype and the commercial service.

The working group developed a property valuation platform with two layers of ledgers. The lower layer allows an individual bank to exchange data with its corresponding set of surveyors only, and the upper interbank ledger enables banks to share information among themselves.

The two layers are logically separated rather than physically segregated. This means that a surveyor can make use of the same node to provide valuation reports to different banks, saving the resources needed for setting up and maintaining multiple nodes.

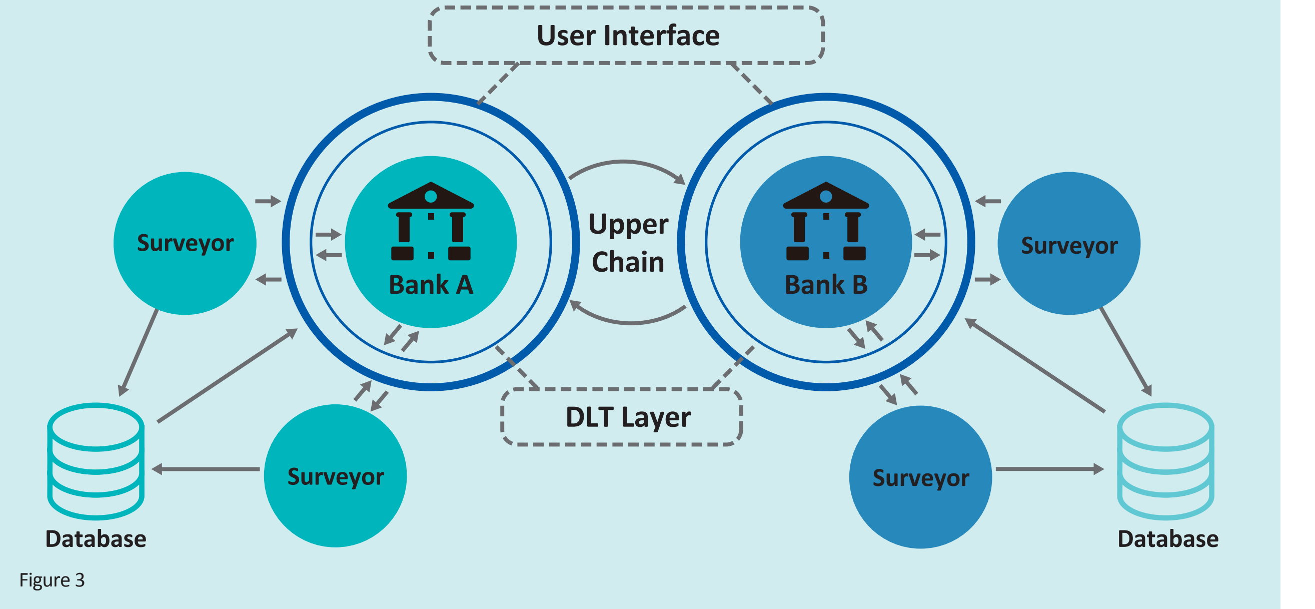


Figure 3

Banks send valuation requests to surveyors through a user interface. The surveyors, upon receipt of any request, submit selected data from the valuation report to the DLT platform via the same user interface, and upload the entire report to a separate database.

Considerations

Since the mortgage loan application prototype is currently the only PoC to have been brought into production, this section discusses the major considerations and challenges encountered during this particular commercialisation process.

Lack of Tools and Utilities

This property valuation platform has been developed based on DLT, a new technology which is completely different from existing platforms. Existing IT tools and utilities for conventional platforms are therefore not applicable for this DLT platform. There is a need to develop corresponding DLT-based procedures, tools and utilities by making reference to existing ones for purposes such as housekeeping, backup and recovery.

Lack of Standards

Other than the lack of tools and utilities for handling the development and daily operations of the platform, there is also no applicable DLT standard. There is a strong need for a reputable and industry recognised authority or body to formulate industry standards for DLT.

Operation and Maintenance

To achieve a sufficient level of confidence in the consensus, tests were conducted to identify the appropriate design of the consensus mechanism. Results revealed that when over two-thirds of all nodes are up and running, the level of confidence achieved is sufficient to validate a transaction.

8.3 Conclusion

All of the PoC work developed in this project shares common issues in areas such as governance, legal and compliance, choice of platform, and data standards. On the technical side, the most significant concern relates to the choice of DLT platform, as which particular DLT platform will ultimately win the technology race is uncertain. Currently, many DLT protocols are not interoperable due to their different underlying consensus mechanisms. The technology community is fully aware of this and is working towards the convergence of network protocols, which may resolve the interoperability issue in the future. On the non-technical side, a major challenge is in achieving collaboration across jurisdictions in different countries, where conflicts between differing laws and regulations need to be resolved. We hope this chapter has provided some practical insights into these issues through its discussion of the real-life implementation of DLT projects.