Whitepaper 2.0 on Distributed Ledger Technology

25 October 2017

Annex

HONG KONG MONETARY AUTHORITY
香港金融管理局

Whitepaper 2.0
on Distributed Ledger Technology

Annex

Table of Contents

Annex A

Trade Finance Contribution

Author
Deloitte Consulting

Proof-of-Concept — Trade Finance

After considering the benefits of deploying DLT in trade finance in the first Whitepaper, the HKMA formed a working group involving five leading banks in Hong Kong, namely Bank of China (Hong Kong) Limited ("BOCHK"), the Bank of East Asia Limited ("BEA"), Hang Seng Bank Limited ("HASE"), the Hongkong and Shanghai Banking Corporation Limited ("HSBC"), and Standard Chartered Bank (Hong Kong) Limited ("SCB"). The working group commissioned Deloitte Advisory (Hong Kong) Limited ("Deloitte") to develop a DLT prototype with the goal of visualising the target operating model and evaluating the feasibility of the technology and its commercialisation potential.

Under the leadership of the HKMA, the working group deliberated on issues of regulatory uncertainty in relation to the operating model, and spearheaded efforts to solve real business problems. Given the scale of the participating banks within the global trade finance market, the working group was able to adopt a global perspective. The Proof-of-Concept ("PoC") work has not just involved the development of a technology prototype, but also a thorough investigation of how DLT can potentially address a wide range of business, regulatory, legal, and technical issues related to trade finance.

1 Introduction

Reportedly, US$16 trillion worth of global trades take place annually, but only one quarter of that amount (US$4 trillion) is financed by banks. Despite this, the World Trade Organization (WTO) has estimated that 80% to 90% of trades actually need financing. Two major reasons for trades not being financed are, first, a lack of trust among participating parties, and second, issues relating to the provenance of the relevant goods. In today's world, a company can use the same purchase order ("PO"), usually in the form of paper documents, to obtain financing from multiple banks by using forged trade-related documents, which are hard to detect. A recent case involved an invoice being fabricated for invoice financing in which a bank lost US$700 million. With banks facing the threat of such enormous fraud losses, many corporates, especially small and medium enterprises ("SMEs"), are unable to obtain financing for their normal operations. This in turn is reducing the total volumes of production and trade in the market.

Additionally, trade finance processes today remain very labour-intensive, involving large amounts of paperwork and a non-standardised workflow. The process of the transfer of assets is opaque, and payments are frequently delayed and error-prone, resulting in very high costs for operating a trade finance business. Those involved in international trade are eagerly looking for breakthroughs that could enable them to cut time and costs in such transactions.

DLT offers a revolutionary solution to improve trade finance fundamentals and boost trade in general. As mentioned, DLT allows all players in the ecosystem to share customer information and transaction histories securely over a distributed data infrastructure, without compromising customer privacy or sensitive business information. The ecosystem participants can be certain of the digitised trading documents being real, and are informed in a timely manner of the progress of the manufacture, delivery and arrival of the goods. Banks can therefore provide working capital financing appropriately along the supply chain.

DLT comes with a feature called smart contracts. Smart contracts allow for the automatic execution of business logics based on specified events. Many events occur throughout the trade finance process, such as the delivery of goods, the issuance of an invoice, and the receipt of payment. These events are currently followed by manual reconciliations and other operational tasks. Smart contracts offer the potential for automating these processes, reducing human error and increasing efficiency.

At the beginning of 2017, the working group formed by the five leading banks and the HKMA decided to ascertain both the business value and the technical feasibility of developing a DLT platform for trade finance. Deloitte was then selected by the banks to be their technology partner. The Proof-of-Concept project was completed in March 2017.

The research project was structured into two streams, a business analysis stream and a technology development stream. The business analysis stream focused on developing the case for business, studying the commercialisation options, and resolving various legal, compliance, data privacy, and governance issues. The technology stream focused on developing an end-to-end prototype using an agile software development methodology.

Intensive discussions were then conducted to collect the key requirements from the major banks. As suggested in the first Whitepaper, the PoC work covered the financing of trade under open account terms, including both pre-shipment and post-shipment financing. Goals included the achievement of the following features leveraging the data distribution nature of DLT:

- To share the status of each transaction along the process to 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.

The five banks actively participated in both the business and technical streams in order to resolve issues relating to data standardisation, process flow differences, interoperability of different technologies, etc. The enthusiasm of the working group members, the capabilities of the consulting partner, and strong support from the HKMA resulted in the great success of the project in a short period of time. Within eight weeks, a trade finance platform was developed with two layers: a presentation layer that illustrated the end-to-end user experience with the platform, and an underlying DLT layer that distributed data across nodes while protecting data security and integrity.

Design and methodology

The trade finance DLT platform leveraged a trade finance prototype developed by Deloitte called "Deloitte Mercury". It was structured in two layers. The underlying layer was for data distribution and consensus facilitation using 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 these were built another layer of APIs specific to trade finance (such as fraud detection mechanisms). These APIs are standardised and can be accessed from a common software library by all DLT network participants.

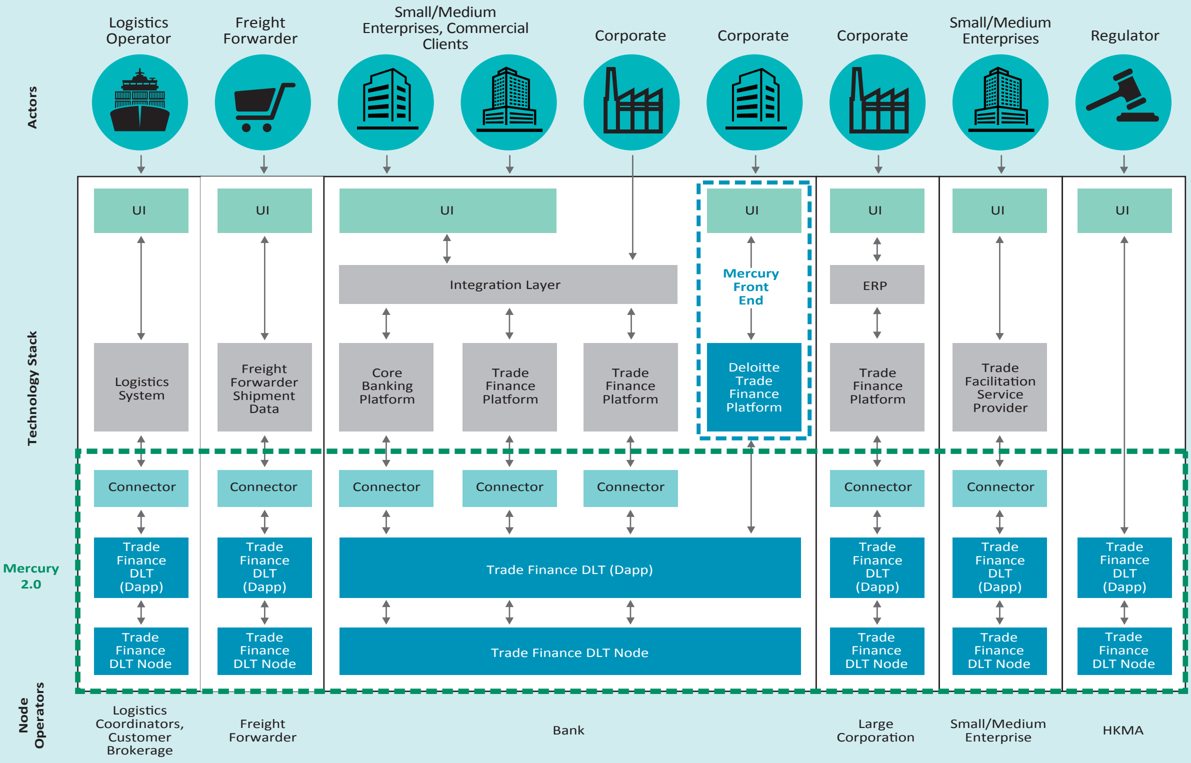


Figure 1: The PoC developed during the research project has two different layers: a layer containing the business logic and an underlying layer with Trade Finance DLT data distribution capability.

On top of the data layer is the user interface and business application layer. It is optional for DLT platform participants to adopt this layer. Large banks and corporates can integrate their own trade finance and trade systems with the underlying data layer without using this application layer. Other smaller players such as SMEs who choose not to be connected via a particular banking portal can use a publicly available trade finance workflow system to conduct business. Government authorities can retrieve real-time data for supervisory purposes directly from the data layer, and will be immune from changes taking place in the business application layer.

The PoC prototype was developed on “Ethereum parity”, a private fork of the public Ethereum. The whole PoC prototype was hosted on the Amazon Web Services EC2 cloud infrastructure, with the application built on an open-source MEANS stack (see Figure 2). MongoDB, AngularJS, and Node. JS were used to develop the business logic and user interface. Through the Web3 module, the application communicates with the underlying Ethereum network through remote procedure calls (RPC).

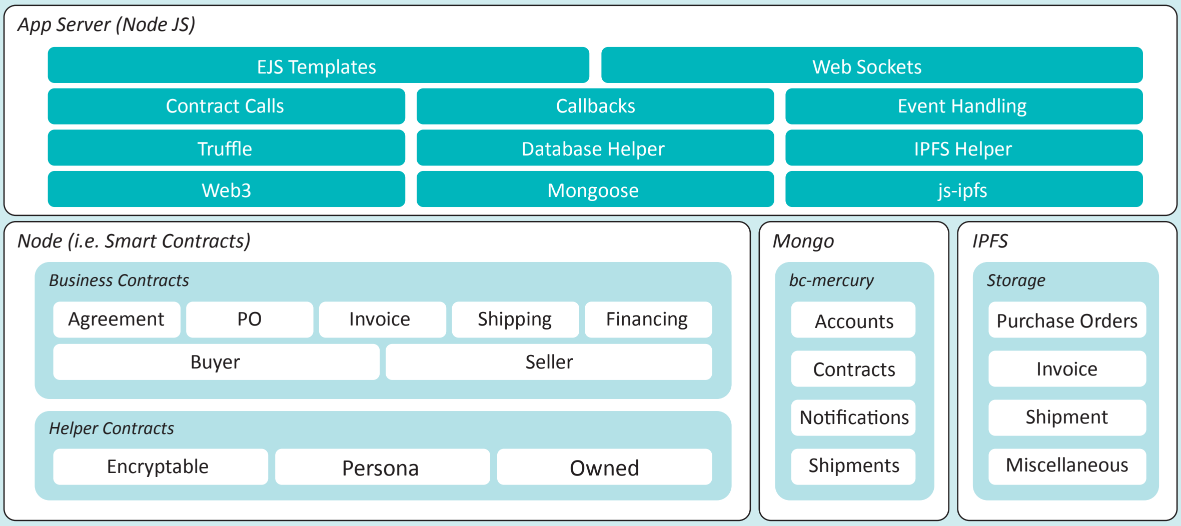


Figure 2: This logical diagram of the network architecture illustrates the underlying MEANS stack of the DLT PoC prototype.

Due to the nature of Ethereum, the consensus mechanism supported was proof-of-work (PoW) or proof-of-stake (PoS). In addition, Passport was used for identity management, while Interplanetary File System (IPFS) was used for document management. The smart contracts were programmed in Solidity.

3 Results and discussion

In the following sections, the results of the three use cases identified in the first Whitepaper are described, and an overview of the perceived benefits given. The chapter concludes with a discussion of some considerations that arose during the research project.

3.1 The use of smart contracts in open account trade

A trade transaction is normally formalised by a PO, which sets out the trade terms on which banks determine when and to what extent financing should be offered to the buyer and seller. The use of smart contracts has two functionalities. The first is to store the various statuses (details in the next section) pertaining to a transaction with a stated data structure so that an enquiry can be quickly made without having to go through the whole trail of records. The PoC prototype demonstrated that smart contracts can indeed reduce the response time for transaction enquiries.

Another use of smart contracts is to distribute event-triggered logic among the nodes hosted by the participants. Finance can be provided to customers more promptly according to the “triggering events” that are built into the smart contract. As a result, transaction transparency is improved and banks can provide financing to customers in a faster and more efficient manner.

3.2 Tracking of trade transaction statuses

The objectives of this sub-use case were to enhance the visibility of the goods and the flow of funds in a transaction, thus lowering the risk of fraudulent transactions or financing. The DLT solution proposed by the working group was to store and share key trade documents and information on the DLT network so they are accessible by all stakeholders in the transaction.

During the PoC work, the working group managed to track 14 statuses in six groups in the Mercury Trade Finance DLT platform:

Group	Status
Purchase Order	Submission
	Confirmation
Pre-Shipment Financing	Application
	Approval
Shipment	Ship Order Submission/Confirmation
	Goods Departed
	Goods Arrived
Invoice	Submission
	Acceptance
Post-Shipment Financing	Seller Application
	Seller Approval
	Buyer Application
	Buyer Approval
Payment	Execution

Table 1: Tracked statuses in the Mercury Trade Finance DLT platform

Features such as shared repository, multiple read-write access, elimination of intermediaries and central authority, as well as timely notifications, were all demonstrated. The status of financing, goods delivery, and payment were tracked and were transparent to participants in the DLT network.

As a result, all participants in the platform have full visibility of the statuses of goods, financing and payments. This transparency means it is much harder to forge an invoice because it is virtually impossible to forge all the other supporting records (e.g. POs and bills of lading) that are digitally signed by different participants. The PoC prototype successfully demonstrated the benefits of adopting DLT in the trade finance environment. First, the improved transparency addresses issues of mistrust among different commercial parties. Second, the PoC prototype illustrates how fraudulent financing, including forged invoices and duplicated collateralisation, can be avoided.

3.3 Matching of invoices to purchase orders

Paper-based processes such as the preparation of invoices require much human effort and are prone to errors, slowing down the trade process. Another issue considered in the first Whitepaper was the fact that the data inheritance feature of invoice preparation, involving the reuse of data from the PO, is only possible if the trade documents have been digitised on the DLT platform.

In the PoC prototype, the reconciliation between the PO and invoices is automated in the DLT network through smart contracts. This is again achieved by using the attribute of smart contracts to distribute event-triggered logic among the nodes hosted by the participants. The reconciliation is not a binary success or failure outcome, but a breakdown of the discrepancy between PO and invoice with a certain tolerance. A similar mechanism can be applied to many other manual processes and significantly improve productivity, cutting time and costs in the supply chain. The reduction of manual processes such as reconciliation is an additional benefit on top of the increase in transparency mentioned in the last section.

3.4 Business values

All use cases and features were demonstrated in the final PoC prototype, and all members of the working group agreed that the results were encouraging and were eager to proceed to an actual pilot of the platform. Further collaboration with other jurisdictions and networks was also initiated, and a wider number of participants, such as trading and shipping companies, were invited to take part.

The participants were convinced of the following benefits:

- **Traders:** Traders, exporters and importers alike have endured a slow paper-based trade process for decades, if not centuries. It has been difficult to track goods, transfer of titles and payments. It has also been difficult to gain trust from financial institutions, especially when the trading counter-party is from another jurisdiction. Without being able to obtain the working capital needed, a trader's production capacity is limited, which in turn affects the overall trade volume in the economy.

  With DLT, traders' identities can be easily validated. Paper trails are digitised and tracking of the trade flow is supported. The cost of conducting business is largely reduced. With a higher trust level, the overall business environment is improved, making it easier for traders to obtain financing and resulting in an increase of trade volumes. Smart contracts also help reconcile POs and invoices automatically.

- **Banks:** Financial institutions face similar problems to the traders. There is no visibility of the goods transfer, and banks often suffer severe losses due to forged documents, fraudulent trades and duplicated financing. These risks increase the need to reserve capital for operational risks, and thus raise the overall cost of capital. Under pressure to reduce their margins, banks are reluctant to offer more credit to the trading community, leading to a substantial loss of revenue uptake.

  With DLT, banks can reduce their operating costs by at least 15%, and sometimes by as high as 60%. They gain full visibility of the trading documents, and can detect frauds without exposing sensitive customer and bank information. With fewer forged invoices or duplicated financing, as well as direct access to trusted sources of trade agreement and performance, banks can be more comfortable with financing SME traders and offer increased amounts of financing. This will eventually translate into more revenue uptake.

- **Freight Forwarders:** Freight forwarders and all types of logistic companies can now easily process trade documents electronically through handheld devices and the Internet-of-Things ("IoT"). DLT allows their clients to monitor the shipment status as well as the authenticity of the shipping locations. This will have important implications in avoiding shipments from sanctioned countries, and detecting vessels that deviate from their scheduled path, among other benefits.

  Another result is that the turnaround time for approval processes and payments will be shortened, resulting in productivity gains and cost savings from document validation and reconciliation. When insurance firms are involved in the future, the transparency offered by DLT will enable usage-based insurance ("UBI"), which will help reduce risks in transit, and eventually lower insurance premiums.

- **Regulators:** Regulators will have real-time oversight as well as an immutable trail of documents throughout the trade finance cycle. Data is standardised for common reporting, and is distributed for access without manual effort needed to extract, format, and consolidate the reports.

The project proved that all the hypothesised business values of a DLT platform for trade finance can be realised, while most issues or concerns can be resolved either through technical means or by business collaboration.

3.5 Commercialisation considerations

Despite its decentralised nature, DLT still requires a set of common rules by which all participants operate in order to ensure its accuracy and trustworthiness. Trade finance is a B2B ecosystem and should be deployed with a permissioned blockchain rather than a public one. Consequently there is a need to design a governance mechanism for onboarding, ongoing operations and dispute resolution. The governance model was discussed at length by the working group. Three options proposed by Deloitte were evaluated for benefits and drawbacks:

- **Working Group**
  A Working Group (see Figure 3) allows decisions to be made through consensus as an association. By definition, a working group is not a legal entity. Each participant owns and operates his/her own node.
  The Working Group is made possible by the distributive nature of DLT. Participating members contribute resources to drive common objectives forward. Each bank provides a representative to negotiate and make decisions on its behalf.

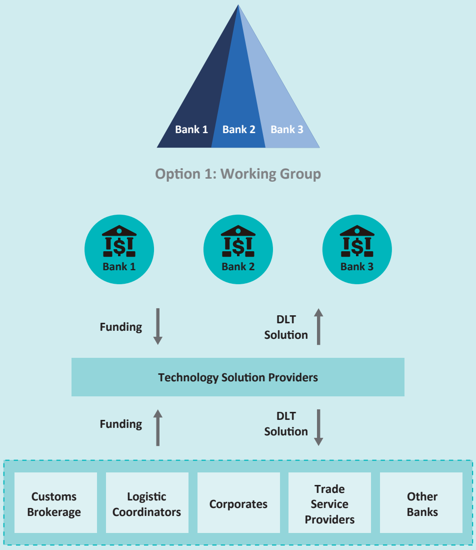


Figure 3: Working Group

Benefits	Drawbacks
High scalability: Amplifies the benefits due to pooled funding while spreading the risk across all parties	Low speed to reach consensus: Takes longer to reach consensus on decisions across participants
Collective ownership: Allows collective ownership of assets developed and hence ensures strategic input by all	Incentive misalignment: Lack of consensus on the strategic direction of the group, slowing down development efforts
Economies of information: Improves sharing of information and decreases the costs and time dedicated to working in silos, and reduces risk of competing efforts that are misaligned with each other	

Table 2: Benefits and drawbacks of a Working Group

Under this model, all banks jointly contribute funding (the contributions need not all be the same) to provide input and design the solution. The solution will be licensed to banks and ecosystem participants that join the network. Individual Working Group participants are responsible for deploying the solution on their own node and for meeting the associated operational and maintenance costs. Intellectual property ("IP") is owned jointly by members of the Working Group; new participants joining the Working Group will not have IP ownership. Individual banks will not be able to capitalise on IP unless this is jointly agreed upon by all banks, i.e. any bank can veto a new pursuit requiring use of the IP.

- **Private Sector Entity**
  Another option is to create a separate, autonomous legal entity that owns and develops the platform (see Figure 4). The platform will be jointly funded by the banks as core stakeholders and offered as a utility to the participants who operate their individual nodes.

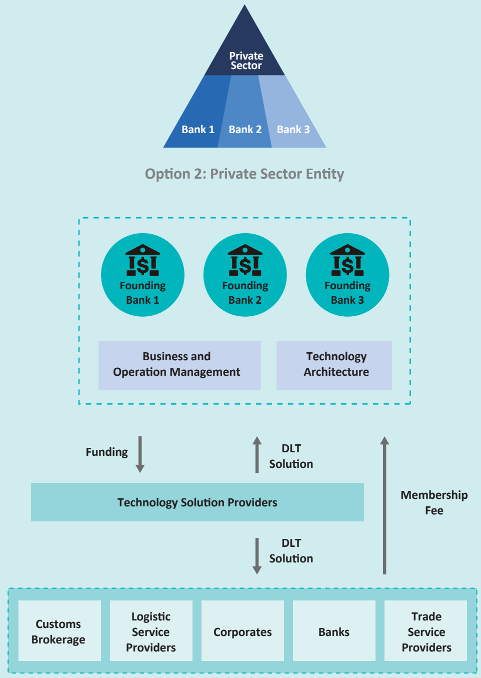


Figure 4: Private Sector Entity

Benefits	Drawbacks
Reduces the risk of project failure: Ensures all parties agree to use the platform before it is built and reduces the risk of building the platform in isolation	High entry barriers: High entry barriers potentially discourage smaller players from joining the DLT platform, depending on the governance model and the way assets are collectively built and owned
Transparent costs: Allows for clear accountability of costs by the entity	
Rapid decision-making: Enables a single, unified process to be devised sooner through this autonomous body, resulting in a cohesion that can generate more value for all participants	

Table 3: Benefits and Drawbacks of a Private Sector Entity

Under this model, each founding member of the entity funds the entity equally. Financial, technological and regulatory costs, as well as revenue and risks, are also shared equally. Solutions are licensed to banks and ecosystem participants that join the network after the formation of the legal entity. The IP is owned by this separate legal entity, not by individual banks.

- **Hybrid Entity**
  Following a close consideration of the first two options, another option was defined which combines their advantages (see Figure 5). This hybrid model includes both the involvement of the public sector, which plays the governance role, and the private sector, which sponsors the development and operation of the platform.

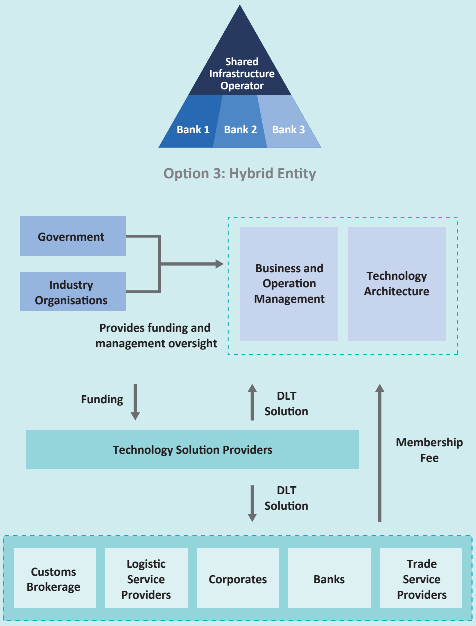


Figure 5: Hybrid Entity

Benefits
Transparency and control: Enables the establishment and adoption of DLT standards based on multiple use cases across the banking industry, as well as high level governance of transparency and full control of the solution
Data governance: Data privacy protection is easily enforced, reducing risk for all participants involved
Cross-border facilitation: Facilitates cross-border cooperation for interfaces and integration

Table 4: Benefits and drawbacks of a Hybrid Entity

The founding banks will set up a funding pool to appoint the shared infrastructure operator to build, operate and maintain the platform. Any risks associated with the technology platform will be managed by the operator. The solution will be licensed to banks and ecosystem participants in the network at a fee that will cover the operational costs. The IP will be owned by the operator.

3.6 On-chain vs. off-chain data

One debate was on what data should be placed "on-chain", and what "off-chain." Proponents of placing all information on-chain argue that this would maximise the value of the DLT network. Opponents identify significant risks associated with this and the negative impact on network performance, as well as noting the difficulties in reaching a common standard among ecosystem participants. A sufficient amount of on-chain data is required to support fraud detection, while too much data on-chain may have an impact on privacy protection, alignment of standards, and platform performance in general. International standards such as UCP600 (Uniform Customs and Practice for Documentary Credits) can resolve some of these data standard issues but not all of them, due to the diversity of the products and services offered by different ecosystem participants.

Whether the data can be accessed by all or only selected participants privy to each smart contract is another topic that needs to be decided on before the underlying consensus mechanism is agreed on for selecting the technology platform. A smart contract is itself software, and raises questions about the ownership of IP. The immutability of the ledger also creates concerns about meeting data retention and housekeeping requirements.

In conclusion, while the business value of DLT has been proven, certain strategic, non-technical issues must first be addressed before the conceptual solution is deployed in commercial production. In order to resolve these issues, it is important to align the technical standards as much as possible to allow maximum synergies, while at the same time preserving a flexibility that allows different participants in the platform to create and maintain different applications on top of the DLT infrastructure.

3.7 Integration considerations

There are numerous types of DLT platforms designed for different problems, and these can be adopted in vastly different ways.

Trade finance is an ecosystem that includes players of very different levels of technology maturity. It includes banks, which are very advanced in trade finance technology, and traders, who often have a minimal degree of automation. The diversity of the landscape means there is a need to design a technology platform that can be adopted by participants in different ways. DLT offers a good foundation, allowing some players to integrate their workflow system with the data layer of the DLT platform, and others to leverage all the business logics embedded in the smart contracts distributed across the network.

By developing a DLT-based trade finance application, major banks, trading companies, freight forwarders, and regulators alike can interact directly with the distributed data nodes of the DLT platform. As for smaller participants such as SMEs, they can access the network through the corporate banking portals of their servicing banks or trade facilitation service providers in Hong Kong. Figure 6 illustrates how participants can interact with the DLT network in different ways.

Apart from integration options, there are questions about which DLT network to adopt as the underlying infrastructure. Due to the current lack of interoperability among different DLT platforms, the research team evaluated various trade finance DLT PoCs from around the world and identified Ethereum, Hyperledger, and Corda as the most suitable protocols. There is an expectation that protocols using a similar consensus mechanism should be interoperable in the near future. In other words, if two networks are both using the Practical Byzantine Fault Tolerance (“PBFT”) mechanism, they have a higher chance of integrating with each other than with networks using Proof-of-Work (“PoW”) for example. The fact that R3 has licensed its Corda source code to the Hyperledger community further validates this expectation. Due to the permissioned nature of the trade finance PoC prototype, the best way to protect one’s investment in the future is to adopt a technology using the Byzantine Fault Tolerance (“BFT”) consensus, while maintaining the portability of the underlying platform across different BFT networks. This is also the reason that the PoC prototype was developed with an underlying trade finance API layer which can effectively shield off the changes from the DLT protocols or networks behind the scenes.

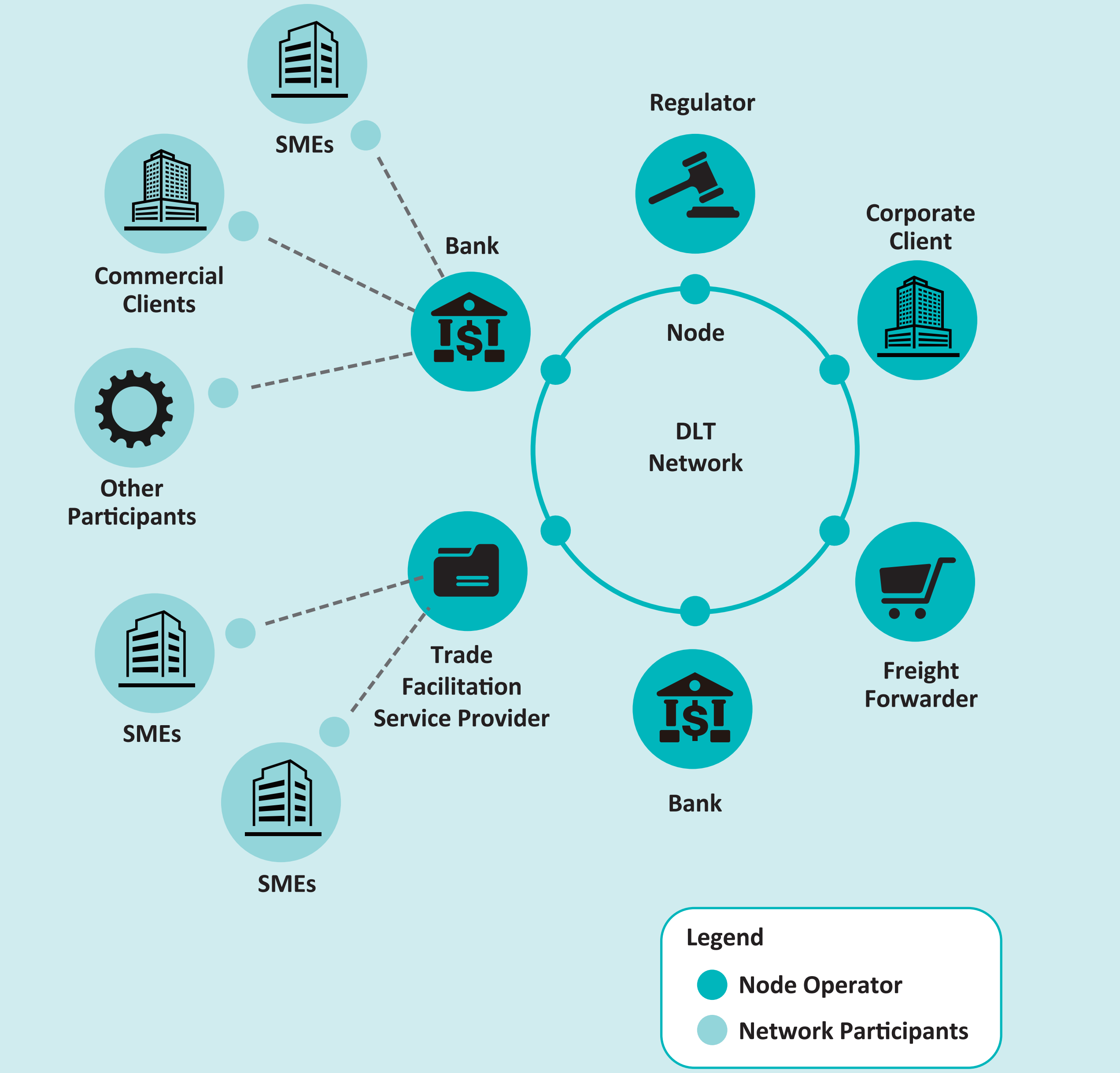


Figure 6: Participants can interact with the DLT network in different ways.

3.8 Legal and compliance considerations

The working group also briefly touched on the legitimacy of the transactions processed on a DLT network. In short, Hong Kong has a sufficient legal framework to support DLT development (for example the Electronic Document Ordinance (Cap. 553)) so that digitally signed contracts are enforceable in the local jurisdiction. A more complicated scenario arises when the transaction is a cross-border one. Laws on international trade apply, but potential disputes are inevitable. Therefore, a neutral and likely public organisation will have to play the arbitration or mediation role should disputes arise. It is recommended that a conflict and dispute resolution committee is established to mediate disputes among participants. A legal framework should also be established, preferably in the form of a legal and regulatory committee, who can also represent Hong Kong in negotiations with other jurisdictions. At the end of day, trade is a cross-border activity. Before smart contracts are widely adopted, legal advice on their applicability and enforceability based on the legal framework of each participating jurisdiction will be required.

DLT allows for different kinds of digital identity management and data encryption. The design options should be evaluated under different regulatory frameworks, and bearing in mind that there may be potential adjustments in the supervision approaches themselves. For instance, regular and after-the-fact reporting may be changed to real-time proactive monitoring. Other common concerns, including the Know-Your-Customers ("KYC") process and Anti-Money Laundering ("AML") regulations, will need to be addressed with different DLT software components.

Another concern relates to data privacy and security. As previously explained, all data submitted to the DLT network can be encrypted with either the traditional private-public key mechanism, or with the SHA-256 hash function built into the DLT network. Both encryptions are very strong and have stood up to numerous challenges in the past decade. As a result, even though data is replicated to all data nodes, and is exposed to the risk of leakage, unauthorised access to the data will not yield meaningful information. Therefore, no breach of data privacy should occur with this hashed or scrambled data even if it is publicly hosted, let alone if it is kept safe in a permissioned blockchain guarded by a formal on-boarding process and rigorous identity management.

3.9 Technology considerations

DLT is a rapidly developing technology. There are many different standards and implementation options, and these require careful consideration in order to protect investments.

The research project and the future implementation have different objectives and thus require different underlying technologies. The goal of the research project was to work quickly and incur minimum costs, so an open source stack was adopted with cloud-based infrastructure. For future pilot and production activities, the architectural design will most likely need to be changed to ensure scalability, security, operability and maintainability.

As for the data structure, an international standard such as ISO 20022 was not fully adopted during the research project, but should be considered as a way to facilitate cross-border data standardisation. The research project only incorporated data required to illustrate the use cases, such as trade status information, invoice information for auto-reconciliation, and PO information for detecting duplicated financing.

Compared to the PoC prototype, the production environment should be built with a more robust technology architecture. Non-functional requirements such as availability, performance and security will require more complex identity management and network typology. Different participants in the network will have different identity management solutions in operation, which will need to be integrated.

Whether key management should be controlled by a central public entity or decentralised to all qualified participants is another area that requires further discussion. Without a centralised host environment, the platform will have to be deployed over a hybrid virtual private cloud (VPC) platform if it is not implemented in the data centres of the individual participants.

A larger concern relates to the DLT network to be used for the future production environment. Currently, many DLT protocols are not interoperable due to their different underlying consensus mechanisms. For instance, proof-of-work (PoW) networks can never integrate with Byzantine Fault Tolerance (BFT) ones. Trade finance, however, requires interoperability by its nature. A survey was conducted during the project to ascertain which technology options for trade finance DLT PoC projects had been adopted around the world. The results revealed that most implementations use one of three different networks: Ethereum, Hyperledger, and Corda, although there is no clear leader in terms of market share.

The technology community is aware of this situation and is working towards the convergence of network protocols. As of today, Hyperledger is already hosting multiple technology options including Fabric, Sawtooth Lake, Iroha, and notably R3 Corda. It is expected that these networks should be able to interoperate in the near future, with some progress to be seen in the upcoming Fabric 1.0. On the other hand, Ethereum is not moving closer to Hyperledger but instead is releasing Enterprise Ethereum of which much is expected. Although the two protocols are both free of charge, they are under different licensing schemes, with the former under Apache 2.0 and the latter under GPL-3. These two technologies are both reaching maturity and will be able to to support enterprise-scale volume and performance. Hundreds of thousands of transactions can be processed within a second with the parallel processing design.
For instance, Fabric 1.0 will come with an ‘Orderer’ which allows multiple sub-ledgers to be stored together for enquiries via APIs. This may potentially resolve interoperability issues in future.

Cross-Country, Different Ledger

With heterogeneous network, data should still be accessed, but smart contracts (logics) will not be executed, hence not updateable, except through APIs.

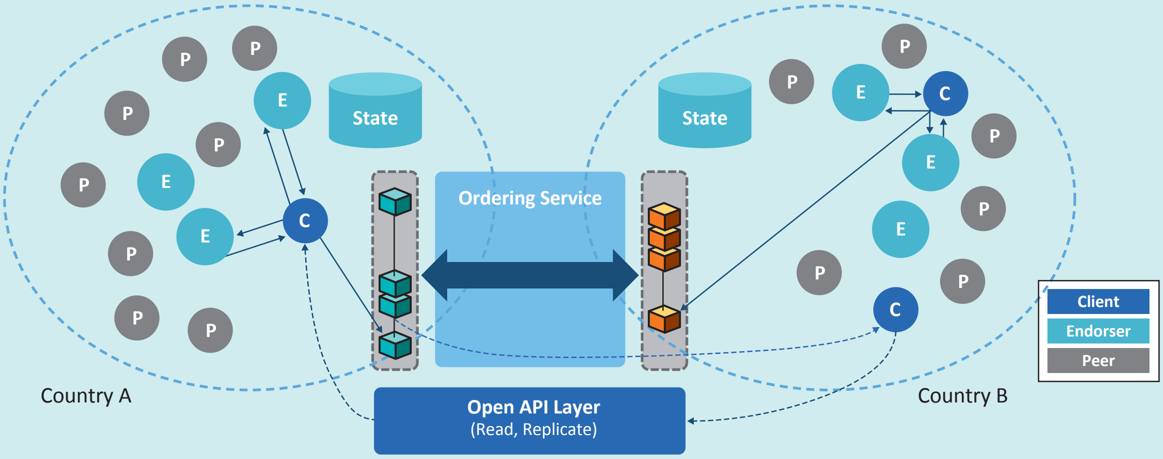


Figure 7: A potential solution to interoperability issues may arrive with the upcoming release of new DLT protocols.

4 Conclusion and recommendations

The key lessons taken from this PoC work can be summarised as follows:

- Adopting DLT provides an indisputable opportunity for the trade finance ecosystem. The potential benefits from cost savings, fraud reduction and revenue uptake are both real and significant.
- DLT allows and indeed demands collaboration between participants in the ecosystem, resulting in a need to develop and agree upon a viable commercialisation model with a proper governance mechanism.
- Many technical concerns, such as those relating to data standardisation, data security and system integration, can in fact be easily resolved with the advance in DLT technology. Once the technology has been fully understood through deep-dive educational sessions, these concerns can be immediately addressed.
- The interoperability of networks across jurisdictions continues to be an issue which can only be resolved by cross-border negotiations and collaboration.

The next step is to move from the PoC work into pilot projects and then commercialisation. Both the commercialisation models and the technology options have been evaluated and a consensus has more or less been reached. Technology is no longer a barrier because of the availability of capable technology solution providers. The integration between legacy platforms and the new DLT technology can also be handled using the latest micro-services architecture. Participants need to form a partnership, select their target product offerings and customer segments for pilot, and start using the platform for a subset of their overall transactions. Once the business benefits have been realised on a small scale, the larger scale rollout should not take long. The last major challenge is collaboration across jurisdictions in different countries, which will rely on the leadership of regulators across the globe.

Finally, DLT and fintech in general is a movement from competition towards collaboration. Those who understand this will gain the most from the development of this technology. People who cling to the old paradigm will soon be disrupted by the new digital economy. Fortunately, major financial institutions, corporates, and regulators in Hong Kong are already embracing not only the technology but also the new paradigm. We are optimistic that we will see Hong Kong continuing to thrive as a major trading and financial hub in the region and the world.

Annex B

Digital Identity Management on DLT

Financial institutions are required to carry out the Know-Your-Customer (KYC) process as part of the on-boarding process before they conduct business with a new client. As the number of regulatory requirements related to the KYC process and Anti-Money Laundering (AML) rules has grown, the incentive for financial institutions to find a cost-effective and user-friendly method to carry out the KYC process has increased. Digital Identity (D-ID) management has been identified as a possible means of streamlining the KYC process, enabling multiple banks to rely on the same shared, secure and auditable source of digitised client information instead of having to collect and verify the information individually and repeatedly.

Author
Hong Kong Applied Science
and Technology Research
Institute Company Limited

1 Proof-of-Concept work

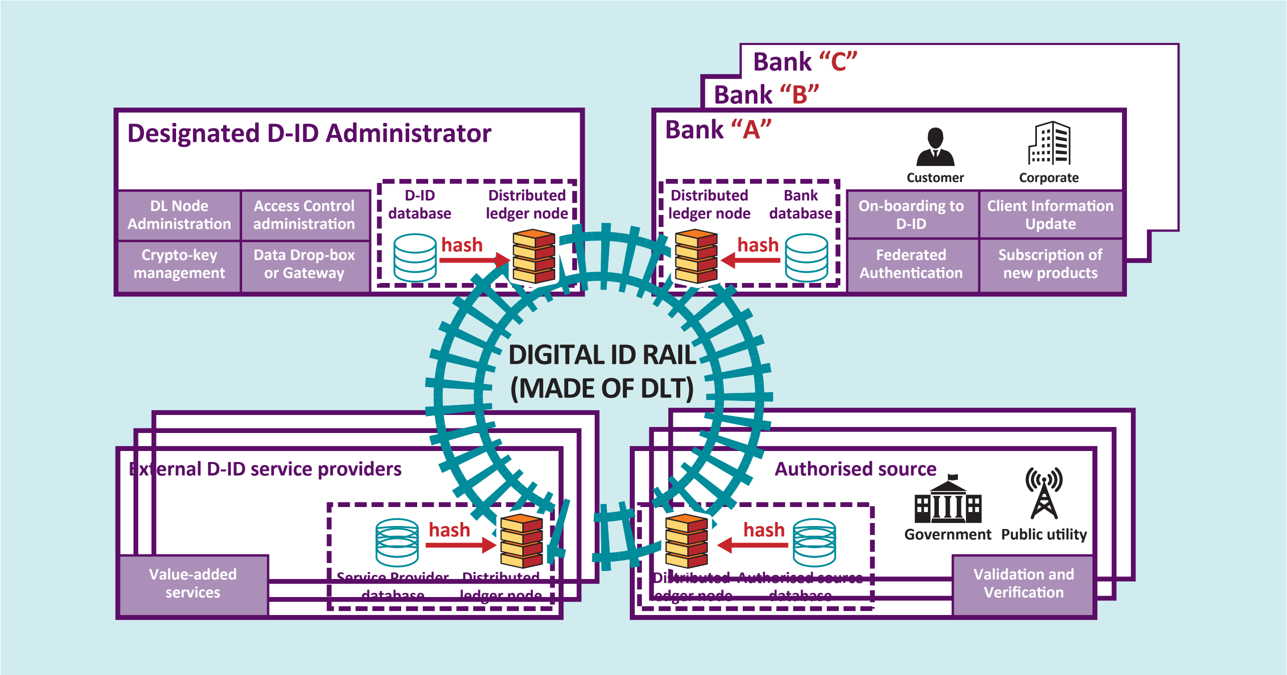
In the first phase of the DLT research project, the HKMA and ASTRI formed a D-ID Working Group with five banks to study the feasibility of applying DLT to D-ID management through a Proof-of-Concept (PoC) project. The Working Group developed the following structure and features for the PoC prototype:

- Selective client information to be stored as immutable and auditable records in the DLT ledger;
- Each of these pieces of data is added to the DLT system through the consensus process among the validating nodes of the participating banks;
- Ledger contents to be simultaneously synchronised in multiple locations served by validating nodes or full nodes, to provide data redundancy; and
- User privacy to be protected transparently through a client-controlled interface relating to banks' accessibility to client data.

Two different configuration options for the D-ID management system are possible:

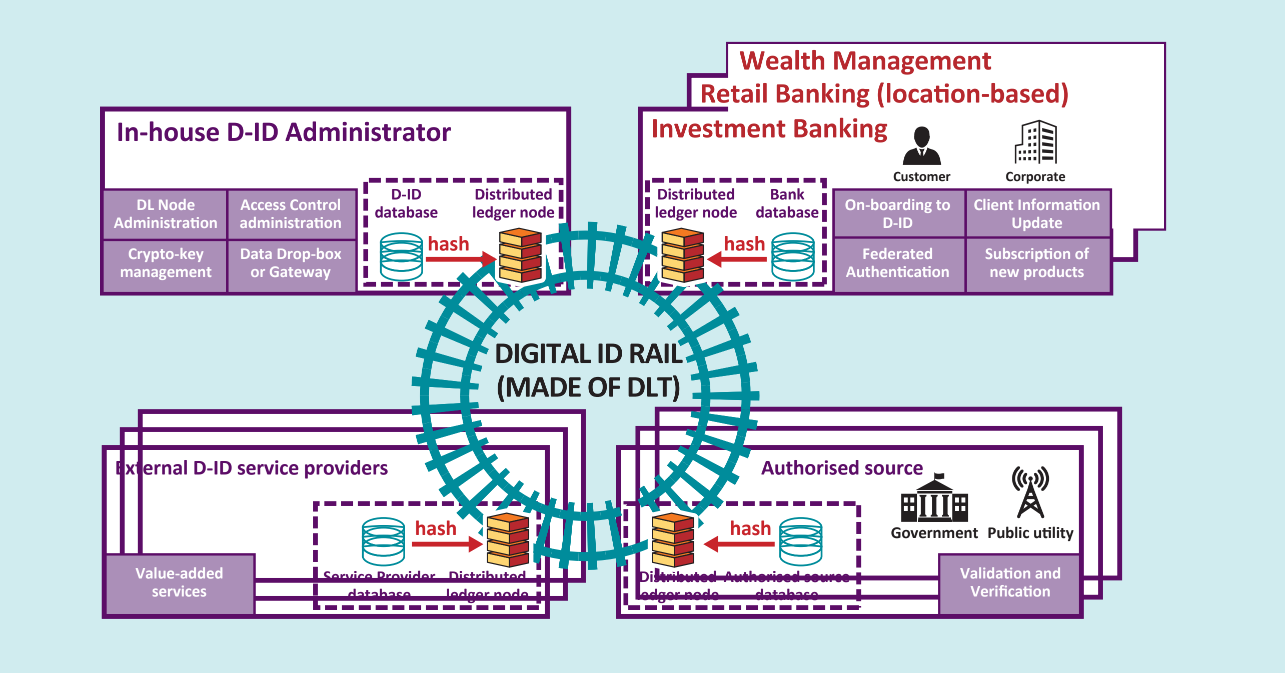
Sector-wide Digital-ID Management on DLT

- Multiple banks could form a consortium with a high degree of collaboration among parties, or jointly subscribe to the same D-ID service provider.



Digital-ID Management on DLT for a global FI

- A global bank could create an internal DLT network that stretches across the jurisdictions and different lines of business in which it operates.



In this PoC work, the first configuration option was chosen because multiple banks are involved in the Working Group.

The system is deployed as a permissioned DLT network, where a membership control policy is enforced to ensure that only registered participating banks and clients may access the system.

When a client first establishes a relationship with one participating bank, on top of the regular on-boarding KYC process, the bank verifies all the client's important identity information (including digital documents) and stores the hashes[1] of this data and the related metadata in a distributed ledger accessible by all participating banks. The data is tagged to a unique D-ID for that client.

If the client later establishes a relationship with another participating bank, the on-boarding KYC process becomes much simpler because the second bank can access the hashes stored in the DLT network, compare them to the hashes of the documents that the client now presents, and confirm the authenticity of the information and documents submitted immediately.

[1] Hash technology is applied to detect any alteration made to the original data. A hash function is a mathematical function that summarises a piece of data, regardless of its size, to a unique fixed-size short data string called a "hash value". Any alteration to the data causes a change in its hash value too, so changed hash values indicate changes in the data record. A common hash function is SHA256, which reduces a data string of any size to a 256-bit number. As the hash function reduces arbitrarily large data to a unique fixed-size short data string, it is often used as a unique identifier of the data itself. At the same time, it keeps the content of the data undisclosed.

2 POC results and findings

The consensus mechanism in the D-ID DLT network makes it possible for banks to collaboratively run and manage the system. This promotes confidence and trust among the participating banks in both the system integrity and the information supplied. This inter-bank synergy helps banks share the burden of client identity verification and reduce the overall costs incurred. Ledger record redundancy, where each bank maintains its own copy of the ledger, not only makes the data more secure, but also makes it more readily available to the bank's staff and to clients.

DLT-enabled ledger transparency eliminates mistrust among banks and encourages further cooperation between them. Both the D-ID information and the full audit history are permanently recorded in the ledger, accessible to authorised members. Banks can access the DLT network to obtain a detailed history whenever necessary.

The DLT-based D-ID system can be connected to KYC utilities to avoid repeated submission of extensive KYC documentation to banks. That way, the KYC process needs to be carried out only once. The DLT-based D-ID system serves as a secure platform on which banks can share their client identity verification information. This reduces overall operation costs because banks can access and rely on the results of client identity verification posted by other banks with a relationship with that client, instead of having to invest manpower and time into repeating the same process.

The following table summarises the benefits of the deployed DLT prototype:

Features	PoC Prototype Details
Streamlines and/or automates processes	• User-friendly applications • API for programme integration
Improves risk assessment and scoring	• Banks share client identity information validation results • Instantaneous notification of identity information changes
Improves service delivery and efficiency	• DLT provides system resiliency
Offers best-fit financial products and services	• Quick access to client identity information validation result
Serves merchants offering non-financial services	• Merchants granted limited access to client identity information validation results

3 Challenges

The Working Group faced various challenges. First, the deployment of DLT-based D-ID in the banking sector requires the presence of congenial settings and support frameworks. It also demands the presence of incentives for banks to share client D-ID verification results within the sector. Legal issues need to be properly addressed with non-ambiguous regulatory policies. Client privacy needs to be protected through both regulatory and technical means. A well-defined client D-ID verification methodology and quality assurance guidelines will help banks gauge the thoroughness and correctness of the D-ID information shared by other banks.

How widely the D-ID system is deployed will be affected by both the level of incentives and the degree of comfort involved for both banks and their clients to adopt this technology.

The performance of the DLT system and its ability to process the daily operation traffic for KYC is another challenge. The volume of traffic is one important factor, but another is the ability of the system to support joint operations by multiple banks. This requires careful selection of the underlying DLT system.

To minimise the effort required to integrate the DLT-based D-ID system with banks' internal KYC systems, we are proposing to have both systems working side-by-side and complementing each other. For example, bank staff will primarily use their existing KYC systems but will be able to obtain additional supporting information from the D-ID system.

4 Conclusion and recommendations

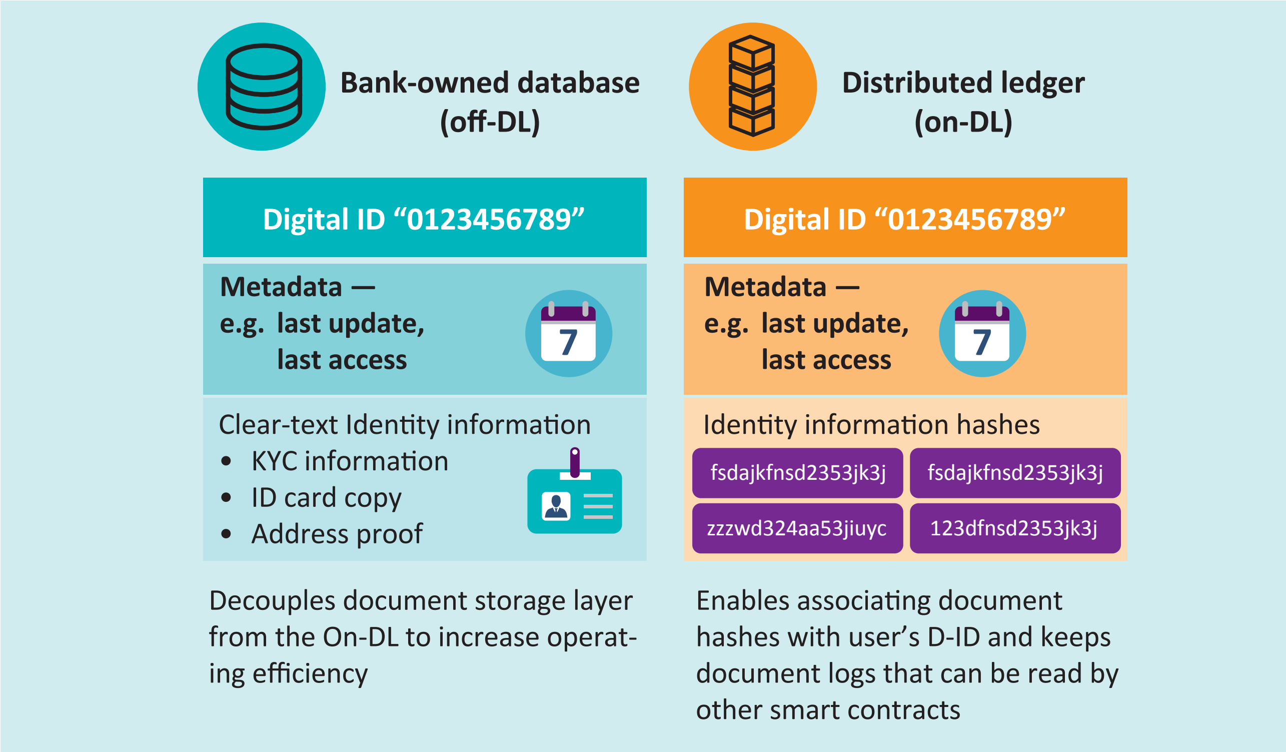
The prototype successfully demonstrates a DLT-enabled D-ID system with the above-mentioned features. Live demonstrations and hands-on experience have illustrated the potential benefits of the system in terms of reducing the amount of effort and improving the quality of the client on-boarding process. The system has been positively received by representatives of the participating banks.

More studies need to be undertaken to determine the technical implementation and the operating model for the D-ID system in commercialisation. This could involve simply adopting the existing DLT solutions, with or without enhancements, or alternatively building a new system. If a new system is to be built, the development could be outsourced to third-party vendors or built through the joint efforts of the participating banks.

Finally, the disruptive DLT technology might also require an appropriate social and legal framework to facilitate and encourage its deployment in the banking sector.

5 Annex – Digital-ID Prototype

(1) Hybrid data storage



Bank-owned database (off-DL)

Digital ID "0123456789"

Metadata — e.g. last update, last access

Clear-text Identity information
- KYC information
- ID card copy
- Address proof

Decouples document storage layer from the On-DL to increase operating efficiency

Distributed ledger (on-DL)

Digital ID "0123456789"

Metadata — e.g. last update, last access

Identity information hashes

fsdajkfnsd2353jk3j fsdajkfnsd2353jk3j
zzzwd324aa53jiuyc 123dfnsd2353jk3j

Enables associating document hashes with user's D-ID and keeps document logs that can be read by other smart contracts

(2) Process-flow

a) First time on-boarding: federated identity

Client needs to visit the bank office to perform first time on-boarding.

(i) Using a phone, the client:

- creates an RSA[2] asymmetric key pair
- submits the public key with a complete set of personal information and documents
- grants access rights to the bank to upload the hashes of client KYC information and documents to the DLT network

(ii) Bank staff submit a request to Identity Manager to create a certificate for client

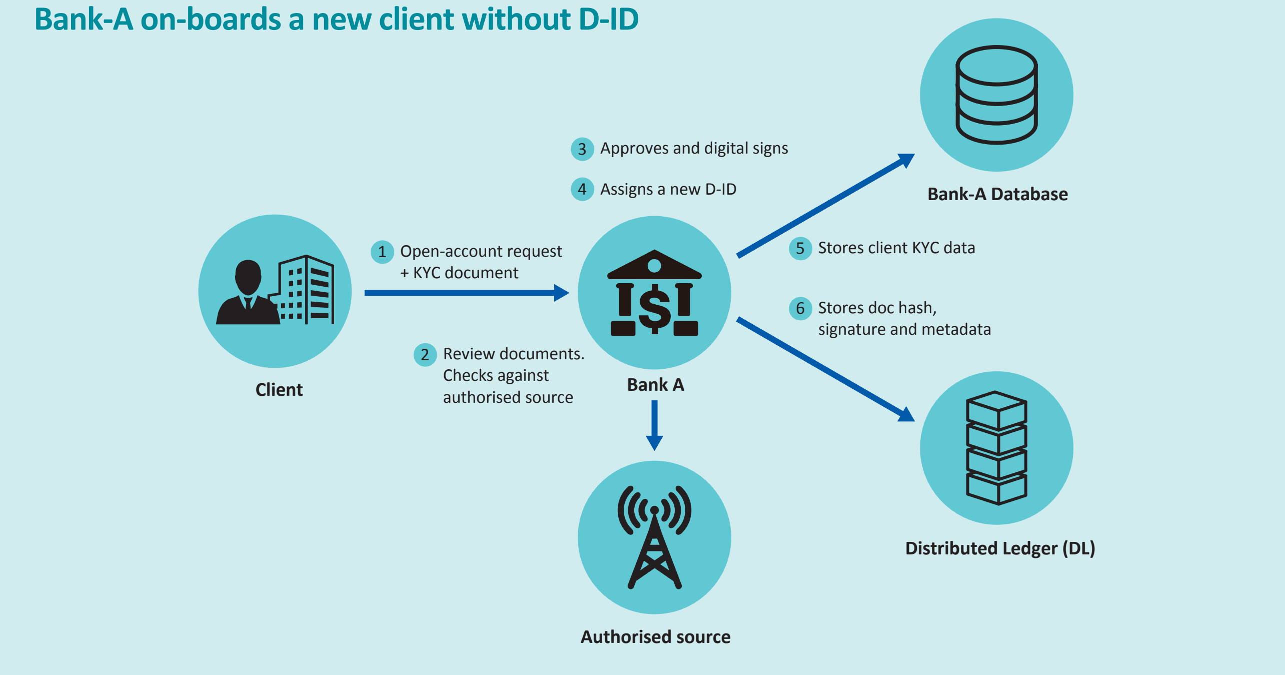
(iii) Identity Manager generates certificate and passes it to client through the bank. The certificate contains client information (including client ID) and client's public key.

(iv) Bank staff verifies authenticity of client information and documents, and after successful verification:

- stores the hashes of the client information and documents in the DLT network
- stores the client information and documents in the bank's private database

[2] RSA was one of the first asymmetric key cryptosystems, and is now widely used. It uses a pair of keys: a public key for encryption and a private key for decryption.

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


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

b) Repeated on-boarding

(i) By phone, the client:

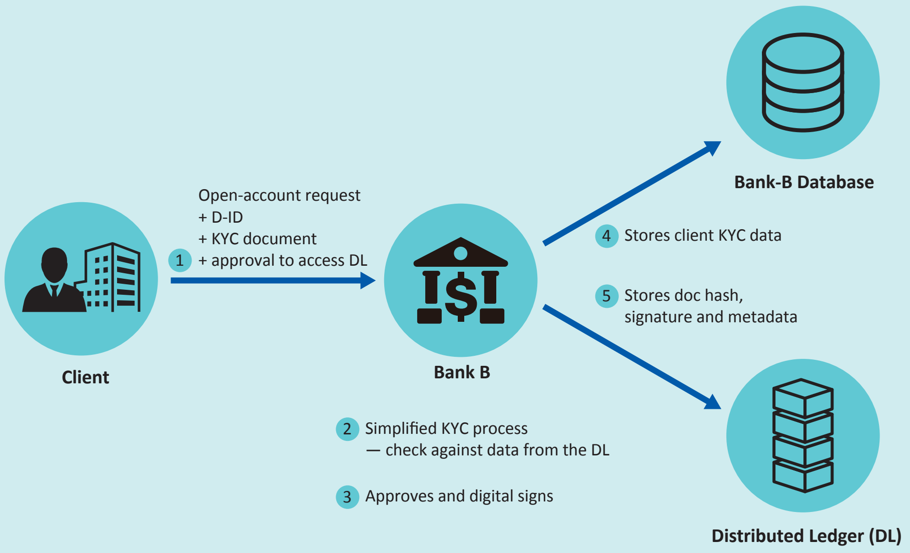
- submits the complete set of personal information and documents
- grants access rights to the bank to retrieve the hashes of client KYC information and documents from the DLT network

(ii) Bank staff accept submitted information and documents only if their hashes are the same as those in the DLT network

(iii) Upon accepting client information and documents, bank staff:

- store client information and documents in the bank's private database
- optionally add a reference log to the DLT network for the corresponding hash entries

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



c) Information update and real-time sharing

(i) Client:

- enters new personal information and document by phone
- visits any bank office and submits the new personal information and documents to the bank by phone

(ii) Bank staff verify authenticity of client information and documents, and if the information and documents are authentic:

- store hashes of the client information and documents to DLT network
- store client information and documents in the bank's private database

(iii) Staff of other banks holding the client's old information and documents will notice the new hash updates in the DLT network. They may do the following to receive the client's up-to-date information and documents:

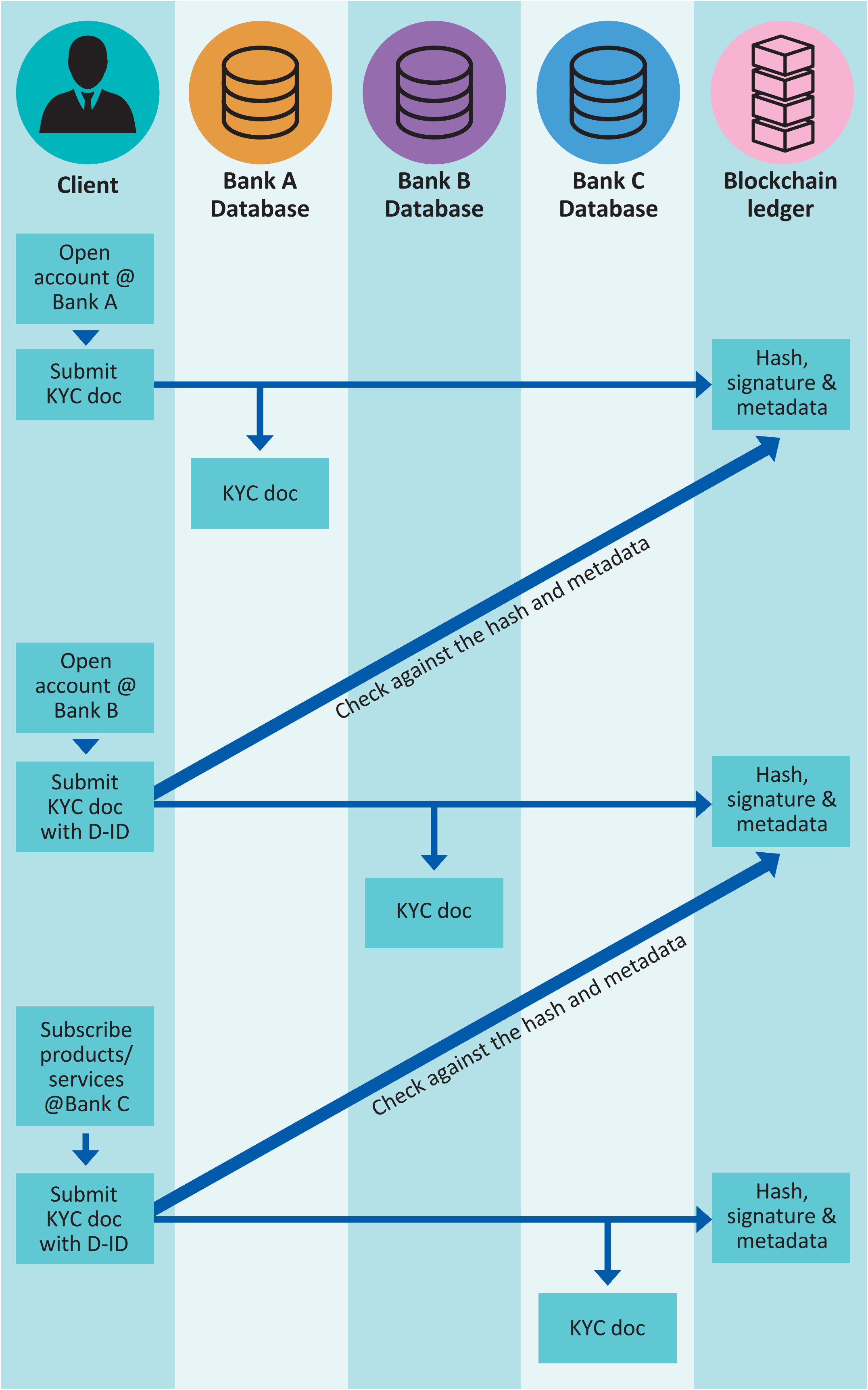
- require client to submit new personal information and documents
- verify the hashes of received client personal information and documents against the new hashes on DLT network
- store the client information and documents in the bank's private database upon successful verification
- optionally add a reference log to the DLT network for the new hash entries

d) Client verifies own KYC information hashes in DLT network

The client may at any time access the DLT network to receive the hash entries of his or her personal information and documents for the following purposes:

- To determine whether the first time on-boarding bank has verified his/her information and documents and uploaded the corresponding hashes to the DLT network
- To determine whether subsequent information and document updates have been verified by the accepting bank and the corresponding hashes have been stored in the DLT network
- To determine which banks have been accessing his/her hash entries on the DLT network

(3) Overall data flow in the prototype demonstration



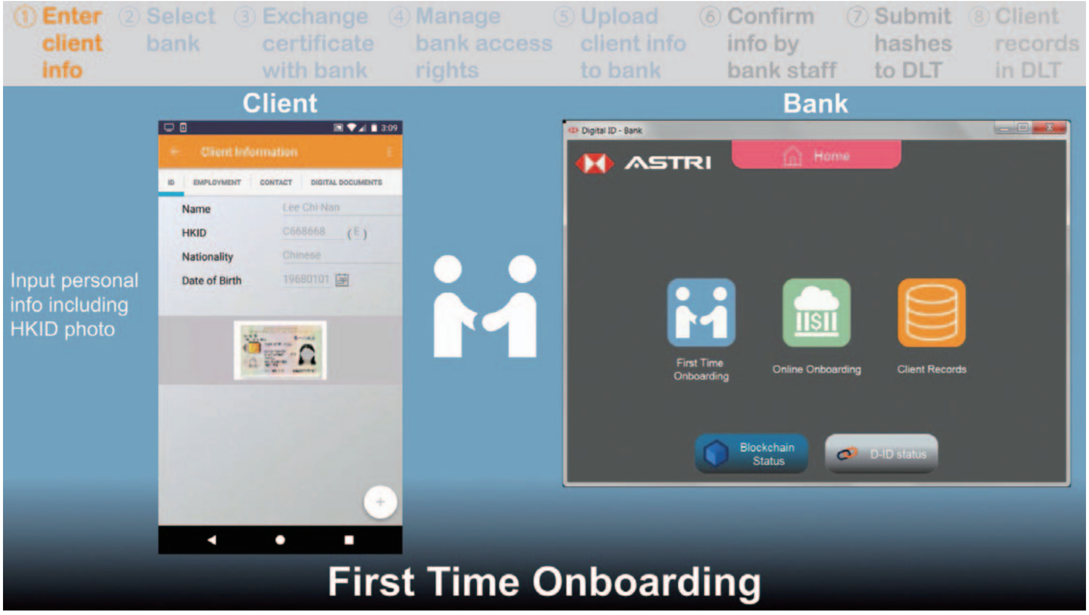
(4) Prototype demonstration

a) First time on-boarding

The client is on-boarding to HSBC Bank for the first time.

Shown below is a prototype demonstration. On the left is the client's mobile phone, on the right is HSBC's computer.

(i) Client sends personal information to HSBC



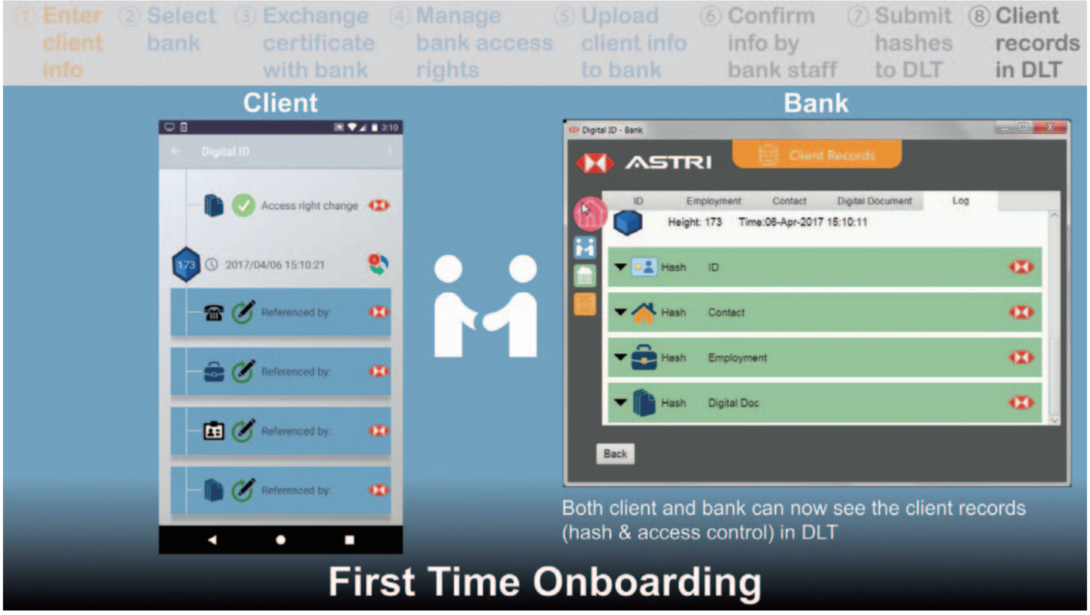
Input personal info including HKID photo

Name: Lee Chi Nan
HKID: C668668 (E)
Nationality: Chinese
Date of Birth: 19680101

First Time Onboarding

(ii) HSBC stores hash of verified client information to DLT ledger

Both client and bank see the hash in DLT ledger.



Access right change

173 2017/04/06 15:10:21

Referenced by:

Referenced by:

Referenced by:

Referenced by:

Height: 173 Time:06-Apr-2017 15:10:11

Hash ID

Hash Contact

Hash Employment

Hash Digital Doc

Both client and bank can now see the client records (hash & access control) in DLT

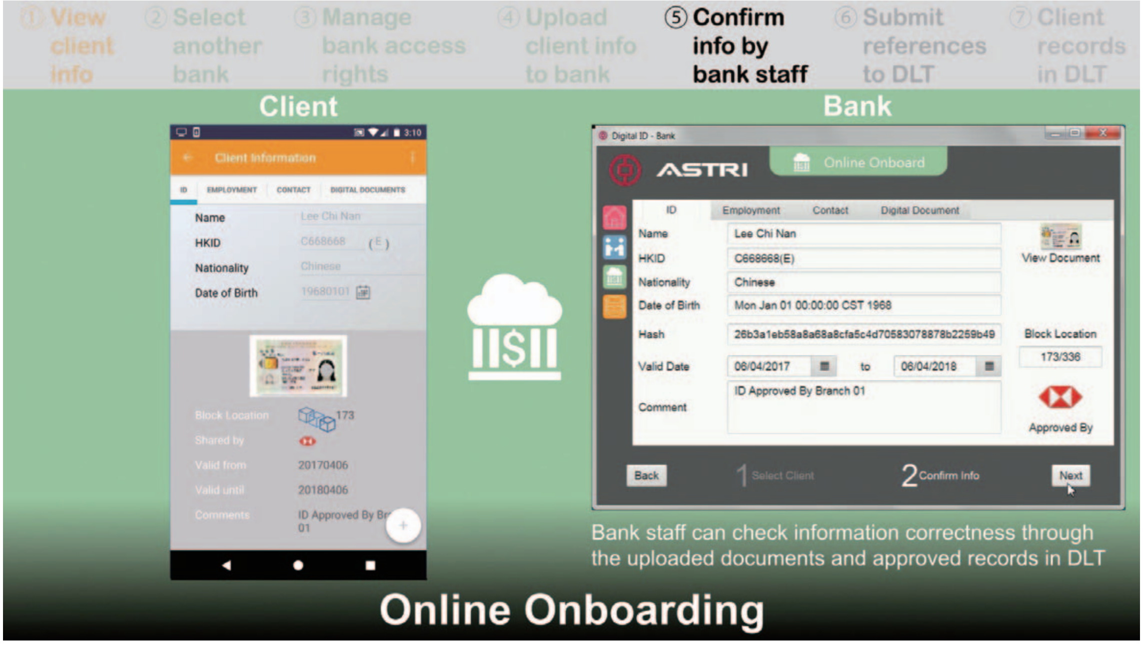
First Time Onboarding

b) Repeated (Online) on-boarding

After on-boarding to HSBC Bank, the client now on-boards to Bank of China (BoC).

(i) Client sends personal information to BoC

BoC sees that the hash of the client’s personal information has been verified and stored in DLT ledger by HSBC. Hence, BoC does not need to perform verification again.



① View client info ② Select another bank ③ Manage bank access rights ④ Upload client info to bank ⑤ Confirm info by bank staff ⑥ Submit references to DLT ⑦ Client records in DLT

Client

Client Information

ID | EMPLOYMENT | CONTACT | DIGITAL DOCUMENTS

Name: Lee Chi Nan
HKID: C668668 (E)
Nationality: Chinese
Date of Birth: 19680101

Block Location: 173
Shared by:
Valid from: 20170406
Valid until: 20180406
Comments: ID Approved By Br 01

Bank

Digital ID - Bank

ASTRI | Online Onboard

ID | Employment | Contact | Digital Document

Name: Lee Chi Nan
HKID: C668668(E)
Nationality: Chinese
Date of Birth: Mon Jan 01 00:00:00 CST 1968
Hash: 26b3a1eb58a8a68a8cfa5c4d70583078878b2259b49
Valid Date: 06/04/2017 to 06/04/2018
Comment: ID Approved By Branch 01

View Document
Block Location: 173/336
Approved By

Back | 1 Select Client | 2 Confirm Info | Next

Bank staff can check information correctness through the uploaded documents and approved records in DLT

Online Onboarding

(5) Client KYC data dictionary

Information	Data Element of Individual
Identify Information	1. Customer name in English and Chinese 2. Identification ID (e.g. HKID and passport) 3. Nationality 4. Date of birth
Employment Information	1. Employment status 2. Employer's name 3. Position/Job title 4. Annual income
Contact Information	1. Address (residential and permanent) 2. Contact number (home and mobile) 3. Email address
Digital Documents	1. Proof of identity 2. Proof of income 3. Proof of address (e.g. bank statement and utility bill)
Metadata on DLT	1. Banks may define any metadata 2. Added by bank when client KYC information hash is collected 3. Additional KYC information can be kept

(6) Security configuration

a) System security — membership only participation

For system security, participating nodes are granted membership certificates by the Identity Manager. Ownership of a legitimate membership certificate is required to gain access to the DLT network.

Ownership of a legitimate membership certificate can only be proven by holding the corresponding private key.

As for access rights, banks with full access rights can read and write information in the DLT network. Some players with read-only access rights can refer to this data on the DLT network.

The visibility of the data will need to be carefully managed so that only participating banks with which a client holds specific accounts will be able to view that client's information.

Annex C

BOCHK Mortgage Loan Application

Author
Bank of China (Hong Kong Limited)

1 Background of the commercialisation of the PoC prototype

Following the publication of the first Whitepaper on DLT by the HKMA and ASTRI in November 2016, BOCHK launched a commercialisation project to turn the property valuation PoC prototype into the first DLT-based property valuation platform in Hong Kong. The objectives of this platform are not only to speed up the property valuation and mortgage loan approval processes, as discussed in the previous Whitepaper, but also to increase the operational efficiency and reliability of this time-consuming, laborious, manual and paper-based process. Developing the PoC prototype into a fully functional commercial platform required thoroughly considering and testing many different aspects of its design, such as the DLT platform and layer infrastructure and architecture, various security issues, and the consensus mechanism. This paper shares the experience gained from the commercialisation project.

2 Platform design

This DLT-based property valuation platform is the first of its kind in Hong Kong. In the application of this new technology, extra attention has been paid to the network and architecture design, especially from the risk management perspective, to ensure the security and resilience of the platform during its actual operation.

2.1 Differences in standards

As DLT is very different from conventional technologies, it was undesirable and indeed hardly possible to deploy DLT using existing IT development tools and standards. Therefore, special care had to be taken when applying existing system standards to the enterprise systems development life cycle (SDLC), the process for planning, creating, testing, and deploying an information system. In practice, implementation has been difficult because different participants have different baseline requirements for security protection. Additional guidelines and information need to be provided for participants to ensure they understand the basic requirements for connecting to the DLT network. All guidelines must be strictly enforced in order to avoid creating unsecured loopholes in any nodes of the DLT network.

Also, due to the lack of standardised housekeeping utilities or tools for DLT, there was a need to develop a customised script for such purposes. Because of DLT's 'no downtime' characteristic, system support and maintenance must be considered across different nodes of the network. It is highly recommended that there should be an operator to take up this role and facilitate the arrangement. For this property valuation DLT platform, BOCHK has initially taken up this responsibility.

2.2 The Consensus Mechanism

In order to achieve a sufficient level of confidence in the consensus, tests were conducted to identify an appropriate design for the consensus mechanism. Some tests relating to performance, stability and cost effectiveness were conducted before the production launch, which revealed that having over two-thirds of all nodes up and running could be considered sufficient for the validation of a transaction. Under such conditions, proper maintenance can be performed from time to time, ensuring the healthiness of the platform.

3 Implementation challenges

Since the launch of the platform, a number of challenges have been encountered. The challenges have come not only from the technology *per se*, but also more commonly have arisen in the areas of governance and control, and in the daily operation, maintenance and administration of the platform.

3.1 Operation and Maintenance

To supplement long-developed SDLC market practice, a new operation and maintenance system had to be established due to the difference between the DLT operating model and that of traditional databases.

For business continuity planning, a DLT platform (like a traditional system) needs to identify a suitable backup and recovery procedure. Traditionally, a disaster recovery (DR) site can be set up by synchronising the data in a peer-to-peer remote copy (PPRC) system, where data stored in the database is duplicated to a secondary site. The secondary site can thus be used for speedy data recovery in case of a system failure in the primary site. As the DLT platform in itself comprises nodes with duplicated ledgers, an additional DR site would be redundant. As a result, a "rolling" backup procedure has been adopted, where another node's copy can be used as backup for the node with system failure. This is one of the most notable advantages of DLT over the traditional centralised system.

However, the challenge comes with the fact that two conditions need to be met before a backup plan becomes feasible. First, in order not to interfere with the normal operation of the system, a sufficient number of nodes need to be up and running. The number of live nodes needs to satisfy the minimal requirement for the DLT network, i.e. having two-thirds of the nodes up and running and a maximum of one-third failed. This should not be difficult to achieve, especially when there are a good number of participants in the platform. Second, although each node carries the full copy of the entire ledger, the nodes are not automatically obliged to serve as backup for other nodes with system failure unless there is a legal agreement for such an arrangement. A proper governance structure would thus need to be set up to deal with this sort of situation.

3.2 System upgrades and change management

The platform should contain adequate governance rules and patch management strategies, especially for security patches, in compliance with both the relevant internal policies of the participating banks as well as the regulatory guidelines. However, there is a lack of appropriate tools and mechanisms to handle system upgrades and change management. For example, ERIS does not provide comprehensive documentation, something which is normally expected from product vendors of an operating system or database. In particular, the system originates from a DLT open source software community (i.e. Ethereum) that as yet has no industry standard. It was therefore decided to adapt the traditional practice for application in a DLT environment. Before conducting an upgrade, a data migration plan must be defined. As for the update itself, it is essential that every single node undertakes it. Hence, the DLT system will be out of service (i.e. offline) during an update.

3.3 IT Governance

From the discussion above on system change management and maintaining a stable ecosystem for adding new participants (e.g. banks or surveyors), it is recommended that a consortium or centralised party takes part in system operations and plans and maintains proper governance for all participants in the DLT network. Taking the admission of a new member as an example, it will be necessary for the centralised party to conduct installation procedures, review network and security considerations and guidelines, provide the hardware and software (e.g. virtual-machine-ware and operating system), and create any necessary documentation.

Apart from having a centralised party for housekeeping, the DLT design should be synchronised between different core members for maintainability and expandability. Since the commercialisation project is based on a permissioned DLT network, its relevant characteristics have to be taken into account, for example its members' different information security policies, system protection requirements and expectations, and practical firewall settings. To meet these requirements, a "Consortium DLT topology" has been established, i.e. the main DLT network comprises different individual DLT networks for each of the participating banks and their individual sets of surveyors. Banks can share specific information with other banks in the interbank network (i.e. the so-called upper chain).

This is to address the surveyors' business model, under which surveyors share one valuation report and the relevant information with only one particular client bank. Another reason is to avoid other participants from taking part in transactions that they are not involved in. Since only essential information is shared in the "upper chain", the DLT platform protects business information.

3.4 On-boarding and access control

The system needs to allow for distinct levels of permission. It must allow users to specify the level of confidentiality for each transaction and to correspondingly conceal identities, transaction patterns and terms of contract from unauthorised participants when necessary. On the other hand, partial visibility is required to allow relevant parties to perform the transaction.

Besides, proper governance guidelines (e.g. regarding authorisation for access to and management of documents for data privacy and auditing) need to be established for off-chain information (i.e. the full property valuation report). The hash value of the document and the key management design grant certain privileges for such access.

To launch the beta version of ERIS, the number of nodes had to be determined while bearing in mind that this number cannot be amended afterwards. However, it would be unwise to create more validating nodes than necessary, due to overhead costs.

Like traditional applications, the read/write access to the DLT layers can be controlled using private and public keys and corresponding key management as a basic instrument, while smart contract features provide even more comprehensive read/write and conditional access controls for the stored data. A different programming language is required to use these enhanced access controls. An alternative approach of maintaining control in the application levels would of course be easier to standardise.

Unauthorised access can also be prevented by firewall controls and by putting an IP whitelist in place.

3.5 Scalability

Due to the distributed nature of DLT, the drawback of extending the nodes (i.e. horizontal scale-up) is that they need to consume additional resources. In addition, consensus among the validating nodes must be well defined once the system is created in order to achieve a sufficient level of validation. The consensus mechanism is proof-of-work (PoW) given that the platform is built on Ethereum. Due to extensive resources consumption, the performance of the DLT network is one major factor that should be considered for the expansion of the network.

3.6 Smart contract language

The features of smart contract language are limited compared to other typical programming languages. For example, blockchain language cannot easily parse, string and store arbitrary format data.

3.7 Legal concerns

Concerns over the intellectual property of the valuation report reinforce the need discussed for access management and document management provisions to avoid unauthorised access.

3.8 Consensus Mechanism

In order to maintain a sufficient level of consensus confidence, an appropriate consensus mechanism (i.e. over two-thirds of validating nodes up-and-running in the DLT network) has been chosen for this mortgage valuation DLT platform.

3.9 Other internal controls implemented

Due to the distributed environment of a DLT network, different participants may apply their own standards and policies when using DLT. This creates challenges for handling certain incidents (such as program defects and mis-cooperation) effectively.

4 Conclusion and Recommendations

4.1 Benefits observed after the launch of the DLT application

For BOCHK, the greatest reward from the project has been that the challenges encountered have ultimately led to a better understanding of how to apply DLT, and have resulted in improvements to the application itself. This process of learning and acquiring deeper understanding is still taking place.

After a successful implementation that focused on developing the application and meeting minimal technical requirements, the next challenge is to find corresponding solutions for the operation issues and IT governance identified. Apart from standard application and network scanning, there exists a particular security assessment methodology for DLT with a cryptographic feature. Ethical hacking to carry out penetration tests is one method of testing security levels in the production environment for which industry references for DLT assessment are insufficient. When moving the platform from PoC work into commercial service, there needs to be a change in mindset involving a focus on the maintenance and governance of the platform and an examination of its architecture and design.

4.2 Future planning for the DLT application

The next steps include extending the functions and features of the implemented DLT platform, exploring other networks (e.g. Hyperledger, Corda, Ethereum) and the possibilities associated with different sub-use cases (e.g. more comprehensive in mortgage-related areas such as e-alerts, trade finance, cross-border payments), and achieving high adaptability of the DLT platform. However, the major task will be to work on achieving interoperability among the participants of the DLT network to maximise mutual benefits.

4.3 Other planning on adopting DLT

Establishing interoperability among different DLT systems is one of the major challenges of the future, but it is also very valuable from the point of view of a globalised financial sector (e.g. international trade finance with Singapore or Mainland China), as it helps to further connect services across different jurisdictions.

Annex D

Six Control Principles for Financial Services Blockchains

Authors
Eoin Connolly
Technical Architect, Deloitte Ireland

Lory Kehoe
Deloitte EMEA Blockchain Lab Leader

Eric Piscini
Deloitte Global Blockchain Leader

Paul Sin
Deloitte Asia Pacific Blockchain Lab Leader

Special Acknowledgements
Guilherme Campos
Senior Consultant, Deloitte Ireland

Niamh O’Connell
Consultant, Deloitte Ireland

1 Best practice – Standard for Blockchain Development

Since its mention by Satoshi Nakamoto in the 2008 whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System", blockchain technology, also called Distributed Ledger Technology (DLT), has gained significant attention in the global financial services community. Researchers and investors are increasingly interested in the transformative and disruptive ability of this technology to:

- Facilitate an exchange of value
- Enable the safe storage of value
- Achieve operational efficiencies
- Secure cost savings
- Increase industry transparency
- Enhance customer experiences

In this whitepaper, we consider three macro factors which we deem paramount to the widespread adoption of private DLTs within the financial community in the long term.

These macro factors are[1]:

1. Governance
2. Law and Regulation
3. Standards

Although this paper discusses each factor in isolation, financial institutions should view all three as interdependent and complementary when considering DLT adoption.

1.1 Governance

The first macro factor is governance. The World Economic Global Risk Report (2017) highlights that a system of structured and effective governance is crucial for all emerging new technologies[2]. To develop appropriate structures for DLT adoption within the financial services community three different governance models must be considered — consortia, joint ventures and statutory organisations.

i) A consortium like structure is where several industry players join together to form a working group to achieve a common goal

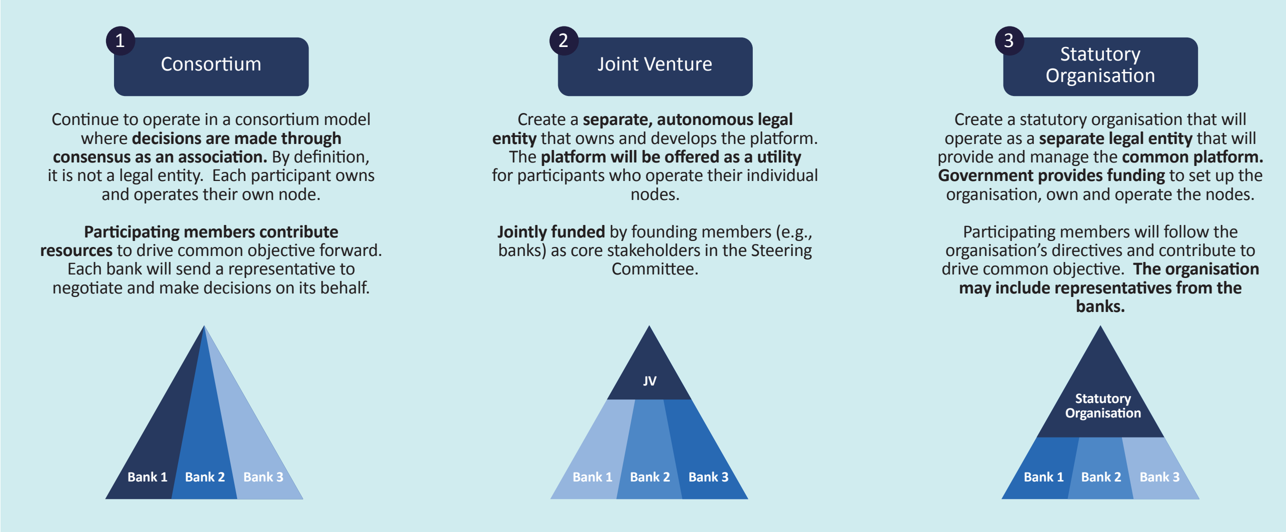
ii) A joint venture (JV) is a separate, autonomous entity established by two or more companies who share ownership, return, risk and governance

iii) A statutory organisation (SO) is a body whose funding and operations are controlled by a regulatory authority.

Depending on the governance model selected, questions may arise on matters such as who engages the independent auditor. In a consortium, the Board-appointed Audit Committee (Board of Directors), or other owners of one member will usually engage the auditor and the auditor will report their findings to this member rather than to each of the consortium members separately. Audit is discussed in more detail in Chapter 3.

[1] De Meijer, Blockchain: How To Make It Operational In Your Company, Nov 2016

[2] World Economic Forum Global Risks Report, Jan 2017



Continue to operate in a consortium model where **decisions are made through consensus as an association.** By definition, it is not a legal entity. Each participant owns and operates their own node.

Participating members contribute resources to drive common objective forward. Each bank will send a representative to negotiate and make decisions on its behalf.

Create a **separate, autonomous legal entity** that owns and develops the platform. The **platform will be offered as a utility** for participants who operate their individual nodes.

Jointly funded by founding members (e.g., banks) as core stakeholders in the Steering Committee.

Create a statutory organisation that will operate as a **separate legal entity** that will provide and manage the **common platform. Government provides funding** to set up the organisation, own and operate the nodes.

Participating members will follow the organisation's directives and contribute to drive common objective. **The organisation may include representatives from the banks.**

1 **Consortium**
Continue to operate in a consortium model where **decisions are made through consensus as an association**. By definition, it is not a legal entity. Each participant owns and operates their own node.

Participating members contribute resources to drive common objective forward. Each bank will send a representative to negotiate and make decisions on its behalf.

2 **Joint Venture**
Create a **separate, autonomous legal entity** that owns and develops the platform. The **platform will be offered as a utility** for participants who operate their individual nodes.

Jointly funded by founding members (e.g., banks) as core stakeholders in the Steering Committee.

3 **Statutory Organisation**
Create a statutory organisation that will operate as a **separate legal entity** that will provide and manage the **common platform**. **Government provides funding** to set up the organisation, own and operate the nodes.

Participating members will follow the organisation's directives and contribute to drive common objective. **The organisation may include representatives from the banks.**

1.1.1 Consortium

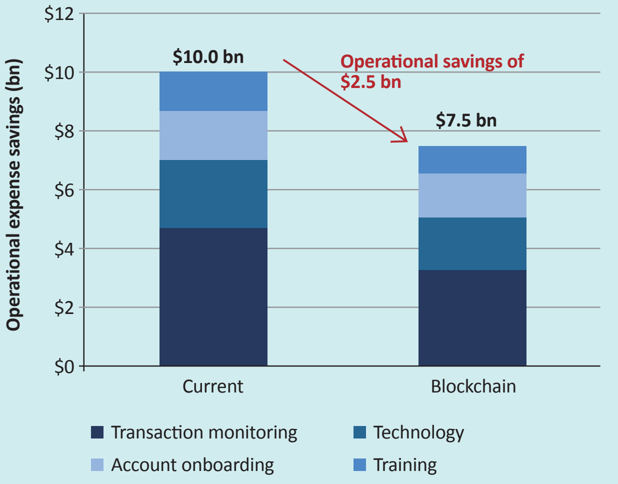
Forming consortia for private DLTs is a popular phenomenon today[3], particularly within the banking sector. Consortium members share setup and maintenance costs, pool resources, perform research and establish the operational and process standards required to implement the DLT solution within their existing infrastructure. Each member has a representative on a steering committee who negotiates and makes decisions on their behalf. A consortium comprising UBS, BNY Mellon and Deutsche Bank recently formed a "Utility Settlement Coin" to facilitate digital cash settlement[4].

[3] Gilbert & Tobin, Blockchain & Shared Ledgers: The New Age of Consortium, Nov 2016

[4] Wiegmann, A, UBS Leads Team of Banks Working on Blockchain Settlement System, Aug 2016

The consortium model works well where a financial institution would benefit from access to shared data. Currently, blockchain-powered Know Your Customer (KYC) utility consortia comprising asset servicers who share the cost of onboarding new investors are being explored in the marketplace. Imagine a world where KYC would only need to be done by one financial institution while other institutions endorse and validate the information and share access to the KYC profile thereby reducing the effort and costs of the onboarding process. According to the "Goldman Sachs Blockchain Putting Theory into Practice" 2016 Report, the banking sector could achieve a 10% headcount reduction and a 30% decrease in transaction monitoring with the use of blockchain technology. The report estimates that the overall operational savings could amount to $2 billion[5].

While consortium benefits such as shared risk, knowledge and IP are attractive, decision making can be time consuming in this governance model and holding specific entities and members accountable sometimes causes internal conflict, particularly in times of uncertainty. This is a business issue that cannot be solved by technology, including DLTs. Consequently, protocols around decision making need to be defined and agreed at the outset to reduce the likelihood of issues occurring in the long term.



Source: Celent, Goldman Sachs Global Investment Research 2016

1.1.2 Joint ventures

Joint Ventures (JVs) are separate entities established by two or more firms, where consensus on critical decisions can be achieved more easily, thus resulting in a faster time to market. Since JVs are considered legal entities, accountability protocols and guidelines are defined at the outset and the probability of internal conflict issues is lower than in a consortium[6]. The JV model focuses on pursuing activities that will maximise financial profitability. This approach works well where multiple stakeholders from different sectors are involved. Trade finance is a practical example: members from banking institutions, regulators and importers and exporters can come together with their associated banks to establish and develop a private DLT. The DLT IP rights are owned by the JV rather than by the parent entities. Profits are distributed equally amongst those members with a stake in the JV.

[5] Gartner, Gartner's 2016 Hype Cycle For Emerging Technologies Identifies Three Key Trends Organizations Must Track to Gain Competitive Advantage, Jan 2017

[6] Lawless, A, A Guide to a Joint Venture in Ireland, Feb 2010 pp. 6

In today's marketplace JVs are being formed between FinTechs and banking institutions. Credit China Fintech recently entered a $30million deal with Bitfury which includes setting up a JV focusing on the Chinese market[7]. This JV has since established a working prototype payment system which includes both P2P lender and payment DLT services.

Currently, consortia and partnerships remain the most popular choice for banking institutions investigating and developing DLT enabled solutions. Blockchain technology is still very much in its infancy and we are unlikely to see JVs formed strictly between banking institutions until they develop stand-alone blockchain capabilities internally.

1.1.3 Statutory Organisation

In the statutory organisation model, participating members (e.g.banking institutions) follow the SO's directives and contribute to common objectives. The Monetary Authority of Singapore Electronic Payment System (MEPS+) is an example of an online interbank payment and fund transfer system that is SO-owned and operated[8]. The benefits of this governance model are twofold: transparency and data governance. The regulator provides transparency, has authority over the process for creating standards and monitoring compliance, and ensures that the standards used are in line with data privacy regulations (PDPO[9]), protecting the rights of all participants with minimal risk. The SO model is a viable option for regulatory reporting. Private DLTs can act as shared data repositories where banking institutions and regulators access and retrieve their financial data. However, these implementations need to be driven by regulators unless banking institutions agree amongst themselves to use a DLT to store and share information, which may subsequently drive regulators to adopt the technology.

1.2 Legal and Regulation

To maximise effectiveness, DLT commercialisation requires an appropriate support framework. Therefore, the second macro factor to consider is the legal and regulatory environment.

Each of the three governance models outlined above will require a legal and regulatory committee. Collaborating with regulated entities within APAC will also be of paramount importance in driving forward DLT adoption and acceptance.

From a technical and legal viewpoint, lack of clarity about the legal enforceability of smart contracts adds risk to DLT implementations within financial institutions. Smart contracts should ideally have the same legal implications as normal contracts and operate in the same way. Real-time obligations, rewards, and sanctions must apply to hold the contracting parties accountable. What differentiates a smart contract from a paper-based contract is that the former is written in a computer executable language and shared on a common blockchain platform without the necessity for a third party. For banking institutions, the positive implications are threefold: enforcement of legal agreements through code, access to a shared immutable data store without the need for an intermediated third-party and the potential to share required raw data with the financial regulator.

However, while smart contracts have the potential to serve as legal platforms, a complex two-step process will be needed to reach this point. Legislation will have to be enacted to define smart contracts as legal tools within each specified region before financial institutions can use them as an alternative to paper-based contracts. In addition, to facilitate cross border activity with other institutions, multiple jurisdictions will need to agree on the same enforceable definition. Achieving this may prove difficult and

[7] Kastelein, R, Blockchain Startup Bitfury Backed For $30m From Credit China Fintech to Expand To China, Jan 2017

[8] Monetary Authority of Singapore, MAS Electronic Payment System, Dec 2006

[9] Lovells, H, An Overview of Hong Kong's Personal Data (Privacy) Ordinance: Key Questions For Business, Mar 2014

costly. In the absence of pre-emptive legislation or a regulatory decision on the enforceability of smart contracts, it is possible that financial institutions in some jurisdictions will not be able to progress with implementations of blockchain technology.

Other considerations in achieving higher quality regulation for private DLT adoption include:

- Cooperation between the joint venture and financial authorities to shape regulations at a regional or global level

- Re-thinking how participants will be regulated, given that regulators could potentially have near-real time access to data via the blockchain. A blockchain doesn't mean a regulator has direct access to each bank's internal system but rather that participants access a shared data source with the blockchain properties of immutability and absolute auditability

- Redefining the regulatory framework when operating in a cross-border model

Where the SO governance model is adopted, it will be imperative to ensure all banks agree with the terms outlined by the legal and regulatory committee. Failing to gain agreement could endanger the success of any proposed solution.

Before investing in a DLT solution, data protection and IP rights should be discussed with legal and regulatory bodies. Protocols and guidelines need to be agreed and designed. In relation to IP rights, a clear definition of who owns the solution is critical to enable DLT development to work effectively. This applies both to the DLT platform (if developed or customised in-house rather than provided by a third party vendor) and to the smart contracts running on it. Defining and agreeing the ownership structure is more difficult where the consortium governance model is used. Regardless of the governance model, however, ownership must be defined in a legally enforceable contract.

In terms of data protection, on-chain data should be limited to a minimal number of fields, whereas off-chain data should be permissioned. This will need to be defined with the DLT protocols independent of the governance model. Additionally, data resilience will have to be considered along with data privacy laws (e.g. PDPO), particularly when discussing distributed file systems for documents. Personally identifiable information (PII) will require special consideration by all parties (e.g., not maintained on the ledger)[10]. Lastly, data retention will need to be factored in to the underlying design of the network for nodes to purge ledger information after certain defined time periods. Where data retention rules apply to individual data sets, destruction of keys used to encrypt the on-chain data should be implemented.

1.3 Standards

The third macro factor in DLT development is standards. These speed up the adoption of technology by financial institutions.

Examples include the 1987 UN EDIFACT standard and the more recent ISO 20022[11] which applies to XML-based financial messages and is used by organisations including the ISDA, Visa and SWIFT.

A proposal for the standardisation of DLTs[12], put forward by the national standards authority of Australia, is currently being considered by the International Organization for Standards (ISO). This group comprises 16 participating countries and 17 observers under the standard ISO/TC 307. Their focus is on standardising DLTs for interoperability and data interchange among users, applications and systems. Their first official meeting took place in April 2017 in Sydney.

[10] Sponselee, A & Aafjes, N, General Data Projection Regulation, Jan 2017

[11] Pupik, J, Explanation: Electronic Data Interchange Standards, March 1997

[12] Ryan, P, Proposal for Standardization of Blockchain and Electronic Distributed Ledger Technologies, Feb 2017

1.3.1 Building Relations with Standard-Setting Bodies

Creating partnerships and building relations with international standard-setting bodies will position an institution as an industry leader enabling them to share input and assist in the creation of upcoming blockchain standards.

These standard working groups can be constituted regardless of the governance model. Financial authorities should consider working with trade and legal organisations in other jurisdictions to form standards and agreements across borders. This will be crucial for the expansion of blockchain across all industries. Irish Funds and Deloitte have established a working group with global asset servicers in Ireland to develop a proof of concept focusing on Investment Fund Returns (Money Market & Investor Funds Returns Reporting – MMIF)[13].

Forming partnerships or working groups with standard bodies makes sense for institutions considering establishing a consortium or JV.

However, for SOs, while standards can be easily created and implemented among participants within a region, cross jurisdictional buy-in is likely to prove difficult to obtain, at least in the short to medium term, as other regulators may not be inclined to be part of a solution that is driven and owned by one regulator.

1.3.2 Adopting Existing Standards and Establishing New Technical Standards

The development of technical standards will give financial institutions a common interface mechanism and facilitate interoperability and scalability at a global level. For example, UCP600 is a common standard or code of practice relating to letters of credit globally[14] while MT798 from SWIFT caters for the import, export and guarantee of letters of credit.

Working with regulators and international bodies is a key step in the development of electronic data standards for DLTs, particularly where guidelines for smart contract management, security and interface protocols are required.

Technical standards for smart contract management will need to cover

- Upgradeability
- Security
- Standardisation of Interfaces

1.3.3 Smart Contract Upgradeability

Smart contracts implemented on a blockchain contain interfaces, business rules and data. All of these elements will change over the lifetime of the platform. It is vital, therefore, that design patterns allow changing individual smart contracts to either add new functionality or remove unwanted or incorrectly functioning features within the application. Code will always need to be changed, even if only to maintain compatibility with new releases of the core platform, and code written to an immutable platform must be capable of being changed to avoid premature obsolescence. Correspondingly, at some future date it may be necessary to migrate data stored in one contract to another. The contract design should always ensure that these data migrations can occur.

1.3.4 Smart Contract Cyber Security

Assuming smart contracts are defined as legally binding contracts, new cyber security controls will be needed to ensure the data is stored and held in a secure environment. However, it is important to realise that most existing cyber security standards will also continue to apply. We will go deeper into the topic of cyber-security controls in Chapter 4.

[13] Gorey, Colm, Deloitte and Irish Funds to Develop regulatory Tech Using Blockchain, Feb 2017

[14] Sebban,G *UCP 600 – El Mercurio*, Sep 2011

It is vital that any code developed for smart contract security adheres to security best practices and is regularly reviewed to ensure that newly discovered security issues are not present in legacy code. Automated tools, if they exist for the blockchain platform selected, are useful in removing some of the manual effort involved in these reviews.

1.3.5 Smart Contract Interfaces

Two types of interface need to be considered. The first is the interface to the smart contracts themselves and the data input and output mechanisms supported to enable data interoperability with other financial systems. Usually this interoperability is delivered by higher-level code wrapping the smart contract, essentially providing a standard interface to the smart contract data. These interfaces can deliver smart contract functionality through diverse methods from secure web services to a fixed-width files in a secure folder.

Where the first type of interface is limited to a particular smart contract, the second interface can be accessed by other smart contracts. Establishing standard interfaces across smart contracts delivers greater system functionality by enabling smart contracts to consume other smart contracts and enhancing blockchain applications with modular functionality in other applications. Examples of this include identity services, tokenised assets (similar to the Ethereum ERC20 standard token interface) and library functions that perform standard financial calculations.

To communicate with smart contracts in a uniform way, specific interfaces have to be defined and developed that meet financial institutions' group requirements. Developing these guidelines and controls facilitates effective and efficient integration with existing systems. This is discussed in more detail in Chapter 3.

To summarise, financial institutions will need to adopt existing software practice standards to ensure DLT solutions are designed, developed and maintained in a secure environment, and comply with industry best practices. New standards will also need to be defined for smart contracts to enable the successful delivery of blockchain solutions into banking and other institutions' existing infrastructure.

2 Interoperability and System Integration Controls

When introducing DLT into the enterprise, it is essential that the DLT system is capable of integrating and interoperating with other systems, including other blockchain solutions or technologies. Even within individual DLT implementations, the blockchain component is likely to be a single part of a larger whole with additional data stores, messaging systems, interfaces and touch points to both internal and external systems. Institutions, therefore, need to ensure all systems are capable of interconnecting and communicating with one another.

2.1 Security Considerations

DLT also presents hurdles to overcome in Hardware Security Modules (HSMs) for key storage and generation[15] and security infrastructure such as Virtual Private Networks (VPNs).

Integration challenges with DLTs are related to their security model which is largely based on PKI (public key infrastructure)[16]. Access rights to write blockchain state data typically requires data transactions signed by a specific private key, while reading blockchain state data requires access to either the ledger file (stored on a number of servers) or access to the interface mechanisms placed over the blockchain data. These interfaces are typically secured via a network credential system (linked to the corporate directory) or a custom password authentication mechanism. These multiple security mechanisms have to work without increasing the surface area for attacks while maintaining the security of a system that potentially contains data from additional companies due to the consortium model which is typical of most blockchain scenarios.

[15] Kakavand, H & De Sevres, N, The Blockchain Revolution: An Analysis on Regulation & Technology Related To Distributed Ledger Technologies, 2016

[16] Allen, C et al, Decentralized Public Key Infrastructure, Oct 2016

2.2 Integration with Legacy Systems

DLT solutions within a financial institution are also likely to require integration with legacy financial systems[17] running on a number of different platforms, such as mainframes, web servers, database servers and more recently web services or RESTful micro services[18].

The issues involved in integrating legacy systems are ongoing for financial institutions. For example, an institution might have a mainframe application that requires a screen-scraping service to provide an automated interface to data while also ensuring that decades of business rules are applied to the raw data as it is entered or extracted from the system.

An issue specifically related to DLTs is the inherently limited data sources that the platform can access, in that the blockchain can only access data stored on the chain. Even on DLTs with smart contract capabilities, such as Ethereum, data sources stored off contract are inherently untrusted (as their data is not part of the single immutable ledger). Furthermore, they must be interacted with via secure mechanisms such as oracles, an interface to the off-chain world from within a blockchain, where all interactions are digitally signed to provide a basic level of accountability. The creation of new oracles to allow smart contracts to automatically pull trusted data from off-chain sources is not a trivial activity although technical approaches such as the Cryptlets within Microsoft's Project Bletchley blockchain framework[19] could simplify and standardise the creation of blockchain oracles.

Most of the integration problems to be overcome relate to DLT infrastructure, security models and the complexities of allowing smart contracts to accept off-chain data sources. Addressing these issues requires a unified security architecture that ties both legacy username and password systems to directory systems and the PKI infrastructure specific to DLTs. It is vital that the most secure component (i.e. the tamper-resistant PKI hardware infrastructure) is not compromised by poor security implementations elsewhere, such as unencrypted password databases, unsecured key stores or open Application Programming Interfaces (APIs).

The functional requirements of blockchain implementations could potentially mean integrating a secure key store service with an internal company user directory or an external cloud directory service that can be accessed by all parties within a private consortium. Another approach could be to assign rights to access functionality predicated on ownership of a certificate installed on user hardware (which still allows for secure machine-to-machine communications) combined with cloud network credentials and corporate identity rules.

2.3 Data Integration

Security aside, integration with DLT systems from a data or interoperability point of view is relatively simple. DLT implementations will typically provide an API which is a common language, such as JavaScript,. NET, Java or Python and such APIs can be used to create a secure RESTful web interface[20] to the blockchain functionality. Most modern programming environments will consume this type of interface which can be used to interact with message queueing systems or service bus applications to provide inter-system operability.

[17] De Meijer, Blockchain: How To Make It Operational In Your Company, Nov 2016

[18] Williams, C, Is REST Best In A Micro services Architecture?, Dec 2015

[19] Grey, M, Microsoft's Blockchain Architecture Overview, Sept 2016

[20] Rodriguez, A, RESTful Web Services: The Basics, Nov 2008

DLT systems provide APIs to read and write data. These APIs can in turn be wrapped in higher-level programming layers (such as a REST API) which can then be used to integrate with an existing Enterprise Service Bus (ESB), or a newly created ESB. Interactions with legacy systems can be routed through the ESB and into fixed-width, or comma-separated files-both common communication mechanisms for systems such as SAP or COBOL mainframes. In addition, batch processes interacting with the REST APIs can load data into other secure data systems, or even centralised data warehouses for centralised management reporting.

These standard integration mechanisms can be used to integrate disparate DLT systems as easily as to integrate DLT systems with more traditional systems. There are additional advantages to blockchain-to-blockchain interfaces as both endpoints have their interactions logged in an immutable ledger. This simplifies and strengthens auditing of interactions.

Given the relative lack of complexity in the interface mechanisms described above, the most important element for a successful and easy integration is the general data architecture of the existing systems and the new DLT. In order to be able to exchange data efficiently and provision all the necessary data, a validated and complete data architecture is essential.

When introducing a new DLT, existing legacy data must be analysed and, where necessary, transformed and loaded into the new system. This is performed following a standard ETL process with appropriate data quality controls:

1. Extract the data from the legacy system

2. Transform it to a format understood by the DLT interfaces

3. Load the data into the blockchain

A specific consideration in blockchain data integration is the technological limitations of some platforms. Therefore, it is important to keep the data structure as simple as possible and only load data that is critical for the blockchain implementation to function. Blockchain read/write speeds are limited compared to traditional databases Off-chain file storage mechanisms such as IPFS (Inter Planetary File System) should be used to store data, with the hashes of the data (and possibly digital signatures) stored in the blockchain to ensure data integrity (or to provide addressing information in the case of IPFS).

2.4 Security Mechanisms

To summarise, security mechanisms are the primary consideration when integrating highly secure, cryptographically-based blockchain security protocols with other, potentially looser access and control rules in existing legacy systems. Integration from a data point of view is relatively straightforward via standard programming interfaces, assuming that the data integration takes place within the established security framework and standard ETL processes. Once blockchain systems have a secure standard interface, they essentially become another enterprise component, albeit with the unique properties of DLT systems-specifically the immutable record of transactions in a decentralised network where peer nodes share data, assets and value.

Blockchains can also be used to secure the data in other systems. For example, database backups can be timestamped onto a blockchain to ensure integrity of the backups for regulatory purposes. Cryptographic approaches such as Merkle trees, make it possible to secure large amounts of data at an individual data row level, rendering it effectively immutable with a single global hash secured on a blockchain.

3. Audit Rules

Will Bible, partner at Deloitte, argues that it is only a matter of time before clients start moving portions of their businesses onto blockchain based infrastructure[21]. The future existence of DLTs will impact how audits are conducted, but it is important to note that blockchains will not entirely automate audits and hence will not make the role of the auditor obsolete but rather it will change some of the processes and approach. Financial and technical auditors will play a fundamental role in assessing the transactional data on the DLT platform as is the case for auditing financial statement and systems today. Although financial data is stored on an online repository, off-chain records upstream and downstream of the on-chain transactions will also need to be audited. In 2017, Deloitte released the output of their investigation into applying professional auditing standards to private blockchain protocols and applications, putting them through both audit and assurance standards to enhance the trust of DLTs amongst their wide client base. The conclusion was that a blockchain platform is unlikely to provide a complete representation of financial statements and auditors will still need to consider evidence and information beyond the blockchain[22].

3.1 The Immutable Record

Data stored on a blockchain is effectively immutable, meaning it cannot be changed or tampered with. On a blockchain, data can only be appended to the existing data set. The immutable audit trail of data stored on a blockchain is an attractive property when considering auditing of blockchain platforms and provides auditors with more readily available transparency over an entity's business activity since a blockchain would be available to interrogate at any point in time without a "closing" process. Another advantage is that in blockchains with cryptocurrency tokens, the distributed ledger can potentially store both the record of the transfer as well as the actual value of the asset at the moment of transfer. This also applies where the transfer is a token representing a physical asset or a more ephemeral asset such as an intellectual property entitlement. However, although both the record and the value transfer are on the blockchain, this does not mean that the auditing can be completed by considering the blockchain data alone. An audit should also take into account any other facts and circumstances necessary for proper accounting treatment of the transaction and factors determining the fair market value of digital or physical assets. It is also important to note that information on the blockchain may not be sufficient to determine the appropriate presentation and disclosures within the financial statement. Further considerations could include identity of the receiving party, rights of the transaction creator to initiate the transaction and ownership rights of the sending party. It might be necessary to identify the connection between a blockchain transaction and an additional off-chain transfer of funds related to this blockchain transaction. The immutable ledger is an important component of the audit and the record being inherently immutable has direct benefits for auditors, but determining elements such as the validity of the data source means that audits must look beyond the blockchain data record.

3.2 Auditing Smart Contracts

Smart contracts also add to the complexity of conducting audits on blockchain platforms. At their heart, smart contracts are code running on the blockchain to ensure the code is processing transactions effectively, as other technologies functional testing would be carried out at design phase. The auditing questions raised by the existence of this code on the blockchain can include:

- Who approves changes to the shared codebase?
- How are access control lists within smart contracts administered?
- What determines the right to access smart contract functionality? Is this access control mechanism consistent across all smart contracts?

[21] Das, S, Big Four Giant Deloitte Complete Successful Blockchain Audit, Feb 2017

[22] Das, S, Big Four Giant Deloitte Complete Successful Blockchain Audit, Feb 2017

- What are the processes if private keys are misplaced or compromised?

- If oracles (off-chain data sources) are used, how is the integrity of the data they provide validated?

Improperly designed and implemented smart contracts can potentially expose the system to security vulnerabilities. This is what happened with the Distributed Autonomous Organisation (DAO) on the public Ethereum blockchain, where a security vulnerability enabled almost half its funds ($60 million at the time) to be withdrawn by an attacker[23]. As smart contract vulnerabilities can enable unauthorised access to the data record, security audits and reviews of the codeaudit rulbase for known vulnerabilities and potential security holes will need to become part of the auditing scope for blockchains. Consequently, security concerns and risk assessments as part of the audit will remain a crucial activity when auditing clients with blockchain implementations.

3.3 Technical Controls

The existence of a blockchain will also not remove the need for technical controls within the organisation. Controls such as the ISO 27001 Information and Data Security standard, will continue to apply[24]. Typical controls organisations adopting blockchain technology will need to follow include:

- Information security policies. Who can access the data? What is the purpose of the platform? How sensitive is the data stored? Are there mandatory data retention and destruction periods? These are only a few of the controls under the information security policy entities would need to address.

- HR security controls. These are the protocols followed to ensure access to the blockchain system is updated when employees leave, or change role, within the organisation.

- Asset Management controls. Developing guidelines to account for ownership of the platform. These can include guidelines to outline ownership of hardware tokens used to store signing keys and laptops with security certificates installed.

- Access controls. Security roles and restrictions and the controls in place to ensure that approval processes and procedures are followed when granting access to create, read, update or deactivate data stored on the blockchain.

- Physical and Environmental Security. DLTs will involve key management. This is likely to include use of Hardware Security Modules, physical security measures such as CCTVs, physical barriers, traditional key security and access controls.

- Operations Security controls. This involves standard infrastructure controls such as virus checking schedules, 0-day exploit remediation, maintenance schedules, capacity and backup management. A distributed ledger node within a private blockchain is still a combination of data and software running on one or more servers, often within a Virtual Private Network (VPN). Standard controls will continue to apply to the operational environment.

- Cryptography controls. These are particularly relevant on a platform where authentication is based on possession of cryptographic keys.

- Information Security Incident Management controls. In the event of a security breach, these controls describe the processes around reporting, escalation and response to the breach and are again critical to ensure safe DLT implementation.

[23] Del Castillo, M, The DAO Attacked: Code Issue Leads To $60 Million Ether Left, Jun 2016

[24] ISO/IEC 27001, Information Technology: Security Techniques, Information Security Management System Requirements, 2016

Note that in a typical shared governance model, establishing a standard set of controls between all parties will be essential.

3.4 Audit Transformation

It is evident that the use of blockchain platforms will not remove audits nor the need for an independent auditor. Rather, it will transform the way in which auditors extract, test and analyse data. Layering blockchain technology with audit analytics could yield standardised, sophisticated audit routines and analysis that enable near real-time evaluation of transactions across the blockchain. DLTs will greatly assist some processes as an immutable data record is a desirable audit feature, but the auditing requirements of the origin of the blockchain data, the integrity of the transactional data and the need to ensure there is a lack of material error from a business, technical and financial reporting perspective mean that there will be a need for a broader group of specialities within the auditing team. Technical specialists will be required to ensure the integrity, accuracy and completeness of the data and the validity of the smart contracts stored in the immutable ledger.

Full scale deployment and adoption of DLTs will force the redesign of some of current auditing practice techniques and procedures. Auditors will need to formulate new rules to ensure safe and reliable DLT activity. Rules relating to data and technological architecture for organisations using DLTs will also need to be defined and agreed during the design phase, particularly if auditors are to use and access such technology to track and monitor financial activity in a legally compliant manner.

Additionally, DLT-based applications will almost certainly be integrated with other non-DLT systems within the organisation, with some of these systems likely to include data feeds from paper-based processes. This means that achieving full process automation for auditing blockchain will not be possible until all connected processes are automated. DLTs enable data structuring and digitalisation, which in turn means management can deploy more automation, analytics and cognitive capabilities over their processes. Having a large proportion of the data and processing on the DLT could also enable the possibility of continuous auditing by designing DLT related software to monitor the ledger and present real-time, high-level auditing information to key stakeholders.

The bottom line is that DLTs will change the way auditors work, and will change the composition of auditing teams to include technical blockchain auditing and cybersecurity specialists, but the technology will not replace the role of auditors today or in the near future and the role of the traditional audit chain will still remain quintessential to the process.

4 Cybersecurity Controls

DLT is intrinsically linked with cybersecurity considerations. The foundation of blockchain technology is private and public key cryptography, digital signing and cryptographic hashes. The ability to write to a blockchain usually requires ownership of a private key that is either in possession of the cryptocurrency tokens or is in an access control list within the platform’s smart contracts. Access can also involve ownership of the decryption key required to read information stored on the blockchain.

Blockchain solutions restrict access to owners of certain cryptographic keys which are used to digitally sign interactions, encrypt and decrypt data and send or receive tokens representing an asset. The security of keys is critical. The ENISA Distributed Ledger Technology & Cybersecurity white paper states that “Stringent policies and procedures must be followed when managing keys, including people, processes and technology.[25]

[25] Enisa, Distributed Ledger Technology & Cybersecurity- Improving Information Security in the Financial Sector, Jan 2017

Breaches involving theft of unauthorised control of these keys can have severe ramifications for a platform using distributed ledger technology. In 2014, a Verizon Breach Report highlighted that only 15% of breaches are discovered within a day, 69% take more than a day to discover and 35% take weeks or even longer.[26] Later in this Chapter, we discuss potential threats to private blockchains but first we need to look at the general cybersecurity challenges facing organisations implementing a blockchain solution.

4.1 DLT Cybersecurity Challenges

Security considerations related to the cryptographic and immutable nature of blockchain technology include:

- Key Management
- Risk of an attacker overpowering a private blockchain
- Centralisation of authority within the network
- Privacy and the right to be forgotten

As discussed in Chapter 2, there are a number of well-established best practices for the storage and transmission of private keys. These involve secure hardware modules and rigorous policies and procedures to ensure that keys are not compromised. There are, however, other mechanisms attackers can use without having access to the private keys.

A denial of service (DOS) attack compromises the ability to process transactions. Where a ledger uses a Proof of Work consensus mechanism, an attacker (potentially an insider in one of the participating entities) could create a disproportionate number of nodes and then reverse blocks and amend historical transactions at will. If each participant in a Proof of Work blockchain is only using 10 nodes, spinning up 1,000 nodes on Amazon or Azure could enable the reversal of potentially 100 blocks. For this reason, Proof of Work consensus is not recommended for permissioned blockchains. Instead, consensus mechanisms such as Proof of Authority or Practical Byzantine Fault Tolerance should be used. Attacks such as the one described are considerably more difficult on a public blockchain as the attacker must overpower tens of thousands of nodes of specialist hardware. This requires a large hardware and power outlay, equivalent to Ireland's total power consumption[27].

Where authority within a network is centralised through a central issuer, authorised participant keys or a single account with the ability to update access rights, compromising this authority can compromise an entire system. Consequently, permissioned blockchain implementations should adopt a paradigm of peers operating in a decentralised network to minimise this possibility.

The right to be forgotten — a requirement to remove data — can be difficult to implement on platforms where data is immutable. In some cases, a blockchain can be pruned to remove blocks older than X years however this approach may not be possible if the data to be removed is intermingled with other data. An alternative approach is to ensure that all data written to the chain is encrypted. When the encryption keys for data to be 'forgotten' are destroyed, the data is rendered unreadable. If this approach is adopted, encryption must be implemented from the outset as later implementation is unlikely to be possible.

Other, more existential, threats to consider include advances in Quantum computing which render core cryptographic components obsolete or damage the integrity of data encrypted with a compromised algorithm. Potentially, this will affect the privacy of data globally. Consequently developments in this field should be monitored and the cryptographic components of systems regularly reviewed to ensure they remain secure and are not compromised by technological advances.

[26] Verizon, 2014 Data Breach Investigations Report, 2014

[27] O'Dwyer & Malone, D, Bitcoin Mining and its Energy Footprint, Jun 2014

4.2 Smart Contracts

Smart contracts bring their own cybersecurity risks. While a blockchain platform with a Turing-complete smart contract language has great capabilities, it also exposes a large security surface area for attackers to exploit, as in the DAO exploit referenced in Chapter 3. The potential for insiders to exploit business rules for their own gain means that controls are required to maintain application integrity.

Code reviews are essential, particularly on platforms where a code vulnerability could compromise application integrity. These reviews should be conducted from a best practices security point of view. Where appropriate, they may include automated review mechanisms to formally validate that code performs the expected functions and is free from known security issues.

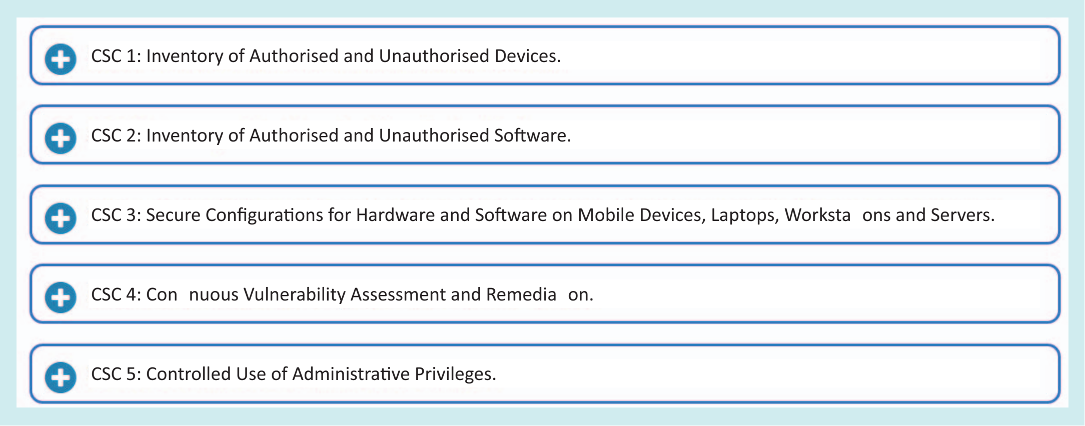
Smart contracts are code running on a shared platform, accessed by all parties,. Consequently, changes to the code affect all entities participating in the chain. When deploying new or updated contracts, a robust governance process must be rigorously applied and followed. Blockchains enable digitally signed consensus mechanisms where DLT participants must review and sign off on new smart contracts before they are activated. In this manner, the blockchain itself enforces internal compliance with agreed controls and procedures.

Standard libraries can also be used to reduce the cybersecurity risks of smart contracts while agreed-upon standard interfaces (such as the ERC20 token standard[28]) reduce the risk of security holes introduced by non-standard implementations of platform functionality.

4.3 Control Standards

Standard controls such as ISO 27001, the Center for Internet Security Controls and SANS Critical Security Controls should implemented as part of a comprehensive cybersecurity control program supported by regular reviews and audits to maintain compliance.

The Centre for Internet Security Controls[29] include:



CSC 1: Inventory of Authorised and Unauthorised Devices.

CSC 2: Inventory of Authorised and Unauthorised Software.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

CSC 4: Continuous Vulnerability Assessment and Remediation.

CSC 5: Controlled Use of Administrative Privileges.

Source: Centre for Internet Security 2017

[28] Frozeman, *ERC: Token Standard*, Nov 2015

[29] Centre For Internet Security, *CIS Controls*, 2017

4.4 DLT Cybersecurity Strengths

DLTs using cryptographic PKI as their security mechanism, are resistant to attackers who are not in possession of the appropriate keys. This, in addition to the shared data and tamper-proof properties of blockchain solutions, means that DLTs have a high level of security. For this reason, provided that controls such as key management follow industry best practices, DLTs are potentially more robust from a cybersecurity perspective than systems which rely on physical or network security or are locked with manually-generated passwords rather than cryptographic private keys.

5 Enhancement of Traditional ICT Protocols

Information and Communication Technology (ICT) encompasses automated means of originating, processing, storing and communicating information, and covers recording devices, communications networks, computer systems and other electronic devices. Management of this infrastructure calls for a specific set of procedures to guarantee that risks related to technology can be identified, measured, monitored and controlled.

As per the HKMA Supervisory Policy Manual on General Principles for Technology Risk Management, ICT controls can be broken down into 5 different categories: security management, system development and change management, information processing, communications networks, and management of technology service providers[30].

The decentralised nature of DLT requires a paradigm shift in the management of these controls.

5.1 Security Management

DLTs rely on cryptography. In Chapter 4 we discussed how this can help overcome security issues related to information protection and user authentication[31].

5.1.1 Information Classification and Protection

Since DLTs are based on cryptographic algorithms, data protection and encryption can take advantage of these functionalities. However, because these systems can, and likely will, connect to multiple external entities where information is shared and available to any participant in the network, encryption needs to become part of the implementation to ensure that data can only be read by appropriate parties[32].

5.1.2 Authentication and Access Control

DLT user access is provided by a public and private key pair. These keys are unique, and once lost, cannot be recovered. Private data on the blockchain will need to be encrypted with the encryption keys for each organisation, which will involve organisations possessing and securing private encryption keys. This need to protect the security of private keys used for accessing the system and decrypting private data means that rigorous processes and procedures must be in place to defend the security of keys.[33]

5.1.3 Security Administration and Monitoring

Decentralisation of systems will require modification of current security protocols. Multiple nodes continuously sending and receiving information from the network increase the risk of unauthorised access. Consequently, it is essential that only authorised users and nodes can perform actions in the system. These parties can be external to the organisation and will need to be monitored accordingly[34].

[30] Hong Kong Monetary Authority, Supervisory Policy Manual : General Principles for Technology Risk Management, Jul 2003, pp.1

[31] Hong Kong Monetary Authority, Supervisory Policy Manual : General Principles for Technology Risk Management, Jul 2003, pp.11

[32] Hong Kong Monetary Authority, Supervisory Policy Manual : General Principles for Technology Risk Management, Jul 2003, pp.11

[33] Hong Kong Monetary Authority, Supervisory Policy Manual : General Principles for Technology Risk Management, Jul 2003, pp.12

[34] Hong Kong Monetary Authority, Supervisory Policy Manual : General Principles for Technology Risk Management, Jul 2003, pp.13

5.2 System Development and Change Management

A further security consideration is that new developments, or changes to current functionalities, will involve multiple external entities. Before a change is applied, all of these entities need to agree. Since developments can be deployed from any node with access to the network, only specific teams or users should be granted permissions to introduce changes. Specific deployment processes for DLTs will be required to effectively address this new way of system development and change management[35]. In addition, system governance will need to ensure that all parties are informed of each proposed release and are prepared to accept the change features.

5.3 Information Processing

Most existing processes for IT operations management support, performance monitoring and capacity planning, and IT facilities and equipment maintenance will apply to DLTs as well. The biggest change will be in disaster recovery planning. We can categorise this into two main topics: network malfunction, resulting in lost connection to the system, and data integrity compromises, which, in a normal situation, would result in rolling back any changes made in a specific time frame.

Losing connection to the network could impact the normal functioning of the system assuming that the outage is more severe than losing a single node. Organisations are expected to maintain multiple nodes in multiple locations to remove any single points of failure. However, in the event of a catastrophic outage, such as internet connectivity being lost across multiple data centres, the disconnected organisation would not be able to participate in any block validations until connectivity was restored and their nodes synchronised with the other nodes in the network. The configuration of the network should ensure that normal operation continues in the event of one of the peers being unavailable. This is why it is important that network functions such as key management or access authorisations are not centralised. Decentralised peer-to-peer systems have high degrees of resilience and this beneficial property of blockchain should be leveraged when creating private networks.

6 Business Continuity Planning and Blockchain

BCP is a subset of risk management. It deals with the risk of an event, such as the loss of critical infrastructure, negatively impacting operations. Disruption of services could lead to lost revenues, additional expenses and reduced profits in addition to potential reputation damage and loss of client confidence.

In a DLT scenario, BCP covers the potential loss of data and processing capability due to loss of servers or connectivity and risks such as cyber-crime. A typical DLT implementation could encompass a wide range of complex technical areas, from key storage and key regeneration in the event of catastrophic data loss to potentially creating new keys if a cyber-crime incident compromised data security.

6.1 BCP Plan

BCP exercises must cover all of the potential threats and risks to a DLT solution. Mitigation processes need to be designed, implemented and, most importantly, tested to ensure business continuity in the event of an incident. Additionally, plans must be updated regularly as new risks emerge.

[35] Hong Kong Monetary Authority, Supervisory Policy Manual : General Principles for Technology Risk Management, Jul 2003, pp.17

For example, a breakthrough in quantum computing could threaten the security of ECC (Elliptical Curve Cryptography) which in turn would involve a move to new cryptographic standards to maintain the privacy and security of the DLT solution. Most DLT cryptographic functionality is built upon standard cryptography (such as SHA-256 hashes or Elliptic Curve Digital Signature Algorithm keys) but there are exceptions using relatively new and untested cryptography such as zero-knowledge proof-based blockchains (Zerocash) or solutions implementing privacy using homomorphic encryption. These developments could result in an extended outage for DLT applications if valid transactions or the privacy of data could not be ensured. Potentially, an event like this could impact the security of the internet in addition to large public blockchains with market capitalisations in the billions. As quantum computing develops, BCP will need to monitor cryptographic advances and vulnerabilities so that proactive responses can be developed to avoid system outages.

In addition to the cryptography risks, other potential risks include loss or theft of private cryptography keys, or encryption of key system data by malware. Crypto ransomware, for example, is becoming a common threat to businesses, with open sourcing of ransomware code and the availability of ransomware as-a-service options, lowers the bar technically. According to Kapersky Labs the number of users encountering crypto ransomware increased by 18% in 2016, with 2.3 million users affected worldwide[36]. Symantec stated that 43% of ransomware victims were employees in organisations[37]. At the time of writing, the WannaCry malware attack has affected hundreds of thousands of computers worldwide in its first few days of operation.[38]

6.2 BCP with PKI

In solutions involving PKI, BCP involves ensuring the technical integrity of the key generation mechanisms (Certificate Authorities, Hardware Security Modules), the business processes involved in the secure transportation of the private keys and the authorisation layer around these mechanisms. In addition, plans need to cope with issues such as redundancy and avoiding data loss or service outage without increasing the attack surface area and effectively reducing operational security. BCP will need to involve internal security teams with possible validation from external specialists to ensure that best practices are adhered to during setup, implementation and testing.

"While proponents of blockchain highlight that it has excellent cyber-security, it has yet to be tested on a wider scale in a highly regulated environment. Exchanges, banks, broker-dealers and fund managers have all been impacted by cyber-crime and regulators require these financial institutions to ensure not only their own cyber protections are fully robust but the cyber-protection measures at their service providers including technology vendors meet these standards" according to Margaret Harwood-Jones in her paper on Blockchain and T2S[39].

6.3 BCP of Network Nodes

When it comes to the blockchain servers and services themselves, BCP activities are simplified by the technology's decentralised nature. A typical blockchain implementation will contain a number of nodes for both redundancy and performance reasons.

[36] Kaspersky Lab, KSN Report: PC Ransomware in 2014-2016 – The Evolution of The Threat and its Future, Jun 2016

[37] Symantec, An ISTR Special Report: Ransomware And Business, 2016

[38] BBC, WannaCry Ransomware Cyber-attacks Slow But Fears Remain, May 2017

[39] Harwood, Jones, M, Blockchain and T2S: A Potential Disrupter, Jun 2016

6.3.1 Public Blockchain Networks

If the blockchain implementation uses a public blockchain network such as the Bitcoin or Ethereum network, then data loss is not possible unless 10,000+ node global networks are also unavailable.

6.3.2 Private Blockchain Networks

If the blockchain implementation uses a private blockchain within a secure environment, such as a VPN, then nodes will need to be geographically separated to minimise the risk of data loss or service outages in the event of a site outage. It is likely, however, given the nature of blockchain implementations that there will be nodes of this private blockchain contained on infrastructure of other companies (such as other financial institutions within the blockchain consortium) and the data will be replicated on those nodes. This minimises the risk of data loss. The ability to recover data by reconnecting to the existing network nodes relies on key management processes that ensure the keys used to authorise access to the blockchain can be recovered or recreated.

6.4 Security Specialists

In this Chapter, we have discussed how some specific concerns and complexities around cryptography and cyber-crime impact business continuity planning. Security specialists, both internal and external, play a vital role in ensuring that processes conform with best practice and keep pace with developments in the cryptography landscape. While traditional BCP concerns about data loss are mitigated by the distributed nature of DLT platforms, solution are usually components of a larger system with traditional databases and web servers. Continuity of service and data integrity of the system as a whole must always be the prime consideration.

Finally, blockchain implementations are not yet common, so there is an additional risk in being a first-mover. This is because the consolidated BCP best practices for the full blockchain solution are likely to be unique within the company and will therefore require a greater level of external validation. Blockchain itself is a new and powerful technology with a small number of reference implementations, but the core aspects of the technology (PKI, peer-to-peer replication, data storage and messaging) have existed in other systems for decades. So while the technology as a whole and the possibilities it offers are new, its components are well understood. Consequently, ensuring high quality business continuity planning for blockchain solutions will mostly involve the collation and aggregation of these existing processes into a unified package.

Annex E

Distributed Ledger Technology Security

Recent advances in an emerging technology called "**Distributed Ledger Technology"** (DLT) have significant implications for the global economy and financial services.

DLT is a set of technologies that through distributed computing and mathematics can now deliver ***Trust*** to an enterprise, consumer or financial institution remotely and without human intervention.
DLT continues to improve at a torrid pace, driven first by Moore's law and second by extraordinary advances in software and connectivity. As technology advances, the rapidly increasing number of use cases being developed on top of DLT are illustrating the transformative potential of the technology to financial services, broader business, economy, and even society.

DLT application in financial services industry has the potential to transform the way value is transferred, information is shared and business logic is coded.

DLT also introduces new challenges. One of the key advantages of the DLT technology over alternatives is the proven strong information integrity security, however, there are many inherent risks related to the confidentiality of information stored in DLT, DLT scalability and availability, as well as the security of cryptographic keys or client software used to simplify user interaction with DLT.

For the DLT to reach its full potential, it must meet or even exceed accepted security standards.

Authors
Marin Ivezic
Cybersecurity & Privacy Services,
Partner, PwC Hong Kong

Kenneth Wong
Cybersecurity & Privacy Services,
Lead Partner, PwC Hong Kong

Kot Tin Gan
Cybersecurity & Privacy Services,
Partner, PwC Hong Kong

Enter the Distributed Ledger Technology (DLT)

DLT is an exciting emerging technology in the financial services industry. It could offer a more effective way to handle a wide range of financial transactions. That seems helpful, but can you rely on it?

Distributed Ledger Technology (DLT) is the generic name for various implementation of blockchain technology solutions. Blockchain is originally the formal name of the tracking database underlying the digital currency bitcoin. The term is now used broadly to refer to any distributed electronic ledger that uses software algorithms to record transactions with reliability and anonymity. This technology is also sometimes referred to as a shared ledger, cryptocurrencies (the electronic currencies that first engendered it), bitcoin (the most prominent of those cryptocurrencies), and decentralised verification (the key differentiating attribute of this type of system).

Given our familiarity with office software and especially spreadsheets, one way to think of a distributed ledger is as giant, interactive, constantly changing spreadsheet that can be viewed by any person that can access it. When one person makes a change, the spreadsheet is updated for all instantly, wherever they are. There is full transparency as to who and when made changes, as everyone that has access to the document can verify them independently.

Key concepts of the DLT:

- The DLT is a decentralised database (or ledger) with predetermined network enforced processes for updating the database for all parties.
- A distributed ledger allows a network to collaborate to form trust and consensus without paying a third party or centralised body to verify accuracy or transactions.
- Taken together, they are a new class of decentralised data structure, which can be applied to disrupt/replace any centralised system that coordinates valuable information.
- These distributed databases are highly transparent, highly available, highly secure, highly trusted, and highly efficient.

At its heart, DLT is a self-sustaining, peer-to-peer database technology for managing and recording transactions with no central administrator or a clearing house involvement and no need for a centralised data storage. Because DLT verification is handled through algorithms and consensus among multiple computers, the system is presumed immune to tampering, fraud, or political control. It is designed to protect against domination of the network by any single computer or group of computers. Participants are relatively anonymous, identified only by pseudonyms, and every transaction can be relied upon. Moreover, because every core transaction is processed just once, in one shared electronic ledger, blockchain reduces the redundancy and delays that exist in today's financial system.

Today's financial institutions are built on a centralised network premise. As banking precedes the digital era, this approach was the only way to tackle the problem of trusted recorded keeping and verifiability. In this model, the bank is the intermediary for all transactions that its customers make, and record the data appropriately.

As we have seen during the financial crises, this model can lead to systematic problems when there is no visibility (or trust) over the holdings each bank has. Similarly, an investor in a Ponzi scheme is reliant on being told by the scheme's operator what the state of their holding is. Bernie Madoff is the central authority.

A distributed system however, by definition prevents this occurrence because everything is visible by all market participants.

DLT could become a game-changing force in any venue where trading occurs, where trust is at a premium, and where people need protection from identity theft. The applications for new products and business models built on DLT are only just beginning to emerge, and already include everything from smart contracts capable of self-execution,[1] to reducing settlement time for corporate syndicated loans,[2] to tracking the progress of assets through a supply chain.[3]

Many of the large banks including Citigroup, Barclays, Deutsche and Santander are investing heavily in exploring its potential, with the later noting that blockchain technologies could reduce banks' infrastructure costs by $15-20bn a year by 2022.[4]

The World Economic Forum (WEF) has conducted a 12-month study[5] engaging industry leaders and subject matter experts globally and has defined six key findings regarding the implications of DLT on the future of financial services:

- DLT has great potential to drive simplicity and efficiency through the establishment of new financial services infrastructure and processes.

- DLT is not a panacea; instead it should be viewed as one of many technologies that will form the foundation of next-generation financial services infrastructure.

- Applications of DLT will differ by use case, each leveraging the technology in different ways for a diverse range of benefits.

- Digital Identity is a critical enabler to broaden applications to new verticals; Digital Fiat (legal tender), along with other emerging capabilities, has the ability to amplify benefits.

- The most impactful DLT applications will require deep collaboration between incumbents, innovators and regulators, adding complexity and delaying implementation.

- New financial services infrastructure built on DLT will redraw processes and call into question orthodoxies that are foundational to today's business models.

The WEF has also identified six key value drivers for DLT in financial services:

- **Operational simplification** - DLT reduces/ eliminates manual efforts required to perform reconciliation and resolve disputes.

- **Regulatory efficiency** - DLT enables real-time monitoring of financial activity between regulators and regulated entities.

- **Counterparty risk reduction** - DLT challenges the need to trust counterparties to fulfil obligations as agreements are codified and executed in a shared, immutable environment.

- **Clearing and settlement** - DLT disintermediates third parties that support transaction verification/validation and accelerates settlement.

- **Liquidity and capital** - DLT reduces locked-in capital and provides transparency into sourcing liquidity for assets.

- **Fraud minimisation** - DLT enables asset provenance and full transaction history to be established within a single source of truth.

[1] http://www.coindesk.com/new-blockchain-startup-brings-contracts-digital-age/

[2] http://www.wsj.com/articles/ex-j-p-morgan-cds-pioneer-blythe-masters-to-head-bitcoin-trading-platform-1426048878

[3] http://radar.oreilly.com/2015/01/understanding-the-blockchain.html

[4] http://www.oliverwyman.com/insights/publications/2015/jun/the-fintech-2-0-paper.html#.VeTMnaBViTM

[5] http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

In a recent response to a call for evidence by the European Securities and Markets Authority Deutsche Bank cited the following areas of potential blockchain application[6] in its letter:

- **Fiat currency payment and settlement.**
- **Securities issuance and transfer** – creation of unique identifiers, transaction tracking and asset segregation.
- **Securities clearing and settlement** – through delivery of more efficient post trade processing.
- **Securities asset servicing** – through automation of dividend/interest payments and corporate actions processing.
- **Enforcing derivatives contract and improving derivatives clearing** through smart contracts.
- **Asset registries** – without the need for a central administrative authority.
- **Know your Customer and Anti-Money Laundering** registries and surveillance.
- **Creating transparency** – and facilitating differentiated customer and regulatory reporting.

There are likely many more – every financial process that involves multiple parties and requires record-keeping could potentially benefit from blockchain.

Deutsche Bank also noted in its letter that the blockchain "**has the potential to create new industry opportunities and disrupt existing technologies and processes**". Beyond finance, it sees the use of the blockchain growing on the institutional level, citing the work of government bodies in the area of the blockchain.

Furthermore, large tech companies are also seeing the potential for blockchain powered products for new and emerging markets, as well as for application to traditional financial and government institutions and processes (such as social welfare distribution, disaster relief fund allocation and voting).[7]

Though it's still early days, what is clear is that we are at the beginning of a revolution in the way trust is delivered and ownership rights (or value) is transferred. On the face of it, this new world does not require third party validation. Society expects better solutions and they are already being realised by those that are applying distributed ledger technologies.

DLT has the potential to disrupt financial services value proposition to customers. Early signs suggest there will be many opportunities to leverage it to help build greater trust in in the exchange of goods, services, assets and information around the world. In our view, DLT may result in a radically different competitive future in the financial services industry, where current profit pools are disrupted and redistributed towards the owners of new highly efficient blockchain platforms.

However, academics, practitioners and regulators have identified several operational, security, governance, privacy and legal concerns and potential risks that should be addressed adequately before DLT delivers on its promise and is implemented for supporting infrastructure as critical as that underpinning financial services.

[6] http://www.scribd.com/doc/273151640/Deutsche-Bank-Letter#scribd

[7] http://www.coindesk.com/microsoft-event-explores-use-of-blockchain-tech-for-social-good-2/

DLT Key Technical Concepts

DLT is a technology that enables so-called “peer-to-peer” transactions. With this type of transaction, every participant in a network can transact directly with every other network participant without involving a third-party intermediary.

Network of Participants

Entities that wish to transact in a standardised way with others can create a network of participants that adopt a distributed ledger technology solution for communicating, storing and validating information related to a single standardised use case.

The DLT innovation is that transactions are no longer stored in a central database, but distributed to all participating computers (nodes), which store the data locally. Traditional intermediaries, e.g. a bank, are no longer required under this model, as the other participants in the network act as witnesses to each transaction, and as such can afterwards also provide confirmation of the details of a transaction, because all relevant information is distributed to the network and stored locally on the computers of all participants.

Blocks and Chains of Blocks

Where a network participant decide to enter data into the distributed ledger (DL) they would define variables of the record as determined by the use case. All information relating to an individual record is then combined with the details of other records made during the same period to create a new block of data.

The data stored in a block is verified using algorithms, which attach a unique hash to each block. Each such hash is a series of numbers and letters created on the basis of the information stored in the relevant data block. If any piece of information relating to any transaction is subsequently changed as a result of tampering or due to transmission errors, e.g. the exact amount of the transaction, the algorithm run on the changed block will no longer produce the correct hash and will therefore report an error.

All number/letter combinations are continuously checked for correctness and the individual data blocks are combined to form a chain of individual data blocks – the blockchain. Due to the interlinking of these number/letter combinations, the information stored on the blockchain cannot be tampered with (at least this would require a great deal of effort). This continuous verification process (called “mining”) is performed by the network participants.

The verification process ensures that all network participants can add to the blockchain but no subsequent revisions are possible. This enables direct, peer-to-peer transactions between persons or organisations that used to require the services of an intermediary in order for their transactions to be legitimately recorded. For example, while a bank is currently needed as an intermediary to effect a financial transaction between two parties, the same transaction can be executed and documented directly between the two parties if a blockchain is used.

A mutual distributed ledger, or a blockchain, has the following key capabilities:

- Mutual – blockchains are shared across organisations, owned equally by all and dominated by no-one;
- Distributed – blockchains are inherently multi-locational data structures and any user can keep his or her own copy, thus providing resilience and robustness;
- Ledger – blockchains are immutable, once a transaction is written it cannot be erased and, along with multiple copies, this means that the ledger’s integrity can easily be proven.

Another way to think of blockchains is as permanent timestamping engines for computer records. Timestamps can be used to prove that data elements were entered at or before a certain time and have not been altered.

In a blockchain the data structure links a unique, computer generated signature, 'hash', of the previous record into a new record. Thus, the mechanism for adding new records must ensure:

- updated blocks are broadcast quickly to all users of the blockchain;
- individual users being unable to access the system does not stop the process of adding new records;
- where there is a conflict such that there are two incompatible versions of the blockchain broadcast at about the same time (a 'fork'), there is a process to ensure that the situation is resolved quickly and the integrity of the blockchain is maintained.

"Permissioned" versus "Unpermissioned"

Oxford Dictionaries define a cryptocurrency as "a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank". Cryptocurrencies – Bitcoin in particular – stimulated the current interest in blockchains, which are a core component of the digital technology making cryptocurrencies work.

A blockchain which can be read or updated by literally anyone, such as a cryptocurrency, is termed 'unpermissioned'. In contrast, a 'permissioned' blockchain can be updated or validated only by authorised users within set governance rules.

Permissioned blockchains need some form of governance that guarantees admission and expulsion from the community of authorised users and defines how updates to the blockchain are made and validated. Permissioned blockchains have a significant advantage in cost and speed. They can also provide an ability to 'evolve', for example providing efficient and timely changes in the structure of the blockchain itself or in supporting processes, as new business or regulatory requirements emerge. Finally, a permissioned blockchain provides a structure for meeting legal and regulatory requirements to 'contract with someone'. In a regulated environment, there may need to be a 'user of last resort' which maintains a current copy of the blockchain and contracts to rebroadcast it if required.

"Public" versus "Private"

A blockchain can also be 'public' or 'private'. A 'public' blockchain is available for everyone to read. Within the 'public' structure, users can encrypt information placed on the blockchain, so that although everyone can see the encrypted version only those who receive the key can actually read the information. A 'private' blockchain is visible only to authorised users.

Blockchain is generally thought of as useful in applications where multiple participants need to agree a regularly changing dataset. However, it can also be useful within one organisation to provide a tamperproof audit trail for external review or to simplify processes between multiple internal areas.

Core DLT security functions

Each block contains two types of information. The first type is application-specific information ('payload') that records transactions or smart contracts. These consist of a combination of data and code executable by the nodes. The second type is internal information that secures the block and specifies how it is chained to another. Blocks get automatically propagated across the network, verified and linked via hash values.

The main protection mechanisms are the following:

The first protection mechanism is linking each block with its predecessor in a way that is computationally hard to undo. This is achieved by the combination of two techniques. The first technique is the use of a hash tree. This means that a hash is calculated for each block, which includes the hash value of the previous block. This is done for each new block created, with the exception of the first block (the 'genesis' block), which has no predecessor. The second technique is the inclusion of a special number in each block, the block's 'nonce'. Insertion of the right nonce allows to calculate a specific hash value over the entire block. Such a nonce is computationally hard to calculate, therefore it is referred to as a 'proof-of-work'. When the correct nonce is inserted in the location reserved, calculating the hash function over the block will yield a specific hash value, i.e. one that starts with a specified number of zeroes. Since the nonce is hard to calculate, replacing a block by another one would mean redoing the nonce computations of all blocks that were subsequently linked to it. With the current state of algorithms and computing power, it is generally believed to be infeasible after extending the chain with approximately six blocks.

The second protection is the peer-to-peer built-in consensus mechanism. A majority of nodes need to agree about the next block that extends the chain. There is no central point of control that can be compromised. A DLT system functions without a central trusted entity, in a peer-to-peer mode, where all nodes are equal. There is no trust between the nodes, so they need to rely on a consensus mechanism to confirm the transactions. The consensus mechanism is based on a verification by every node that the received information complies with a set of rules, and by a verification of the nonce (the 'proof-of-work'). The rules verify that the proposed transaction complies with the application functionality. This is application-specific. For example in the case of a virtual currency it is verified that the payer has ownership over the coins he wants to spend.

Such ownership is demonstrated by a signature using the private key of a Public Key Infrastructure (PKI) key pair. The verification of the 'proof-of-work' demonstrates that a node has invested the required computational power to participate in the extension of the chain.

If two nodes would broadcast different versions of the next block at the same time, some nodes may receive one or the other first. Each node would work on the first block received, but save the other branch in case it becomes longer. The tie will be broken when the next nonce is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

While these two protection mechanisms are inherent to each DLT, the third protection mechanism is optional. It stems from the fact that DLTs come in two different flavours: previously discussed permissionless and permissioned. The third, optional protection mechanism is designing the DLT application to use the permissioned model and allow only a limited set of known and accepted network participants, or nodes, to process the transactions and extend the chain. As this type of chain is typically set by know and consenting organisations with assumed level of trust, the consensus mechanism could be based on a less intensive computational processes than the previously described 'proof-of-work'. Such permissioned DLT function is based on the self-interest of the participants and they do not need to prove each other they invested sufficient amount of computational power in confirming the transactions.

Regulatory Point of View

Regulators have initially monitored many DLT-related initiatives and there are examples where enforcement actions were taken against projects that were clearly in breach of the current legal framework. After the initial wait-and-see stance, regulators have become convinced of the possibilities of the technology since it has the ability to achieve a more accurate way of reporting and increase regulatory efficiency. DLT could offer the regulators access to a vast amount of records and ultimately alter the way the industry is regulated. It has already shown that this has the ability to reveal money-laundering schemes or potentially discover unauthorised international tax avoidance in a quicker way.

This increased interest in the DLT by the regulators was noticeable by the amount of reports and guidance that were published in short succession. For example, the European Securities and Markets Authority (ESMA) has recently closed off a period for a call for evidence on investments using virtual currencies or DLT and the European Banking Authority (EBA) has set up a task force to investigate DLT implications. These and others actions are to be welcomed and show of some appreciated well-willingness from the regulators' side.

In addition to the growing number of publications and on-going research, there are now regulators actively facilitating DLT projects. For example, the State of New York is offering a 'BitLicense' which allows businesses to conduct virtual currency activities on a DLT-infrastructure. In the UK, the Financial Conduct Authority (FCA) has set up a regulatory sandbox to provide innovative initiatives with a so-called 'safe space', i.e. businesses can test their products and services in a way they do not have to worry about regulatory constraints or be afraid of legal action taken against unauthorised activities. Similar to the UK, the Australian government is taking a leading role in providing start-ups with facilities to further develop their activities with assistance from for example the Australian Securities and Investments Commission (ASIC). Adding to that, the Reserve Bank of Australia (RBA) is developing their 'New Payments Platform' (NPP) by implementing DLT. This will provide, amongst others, real-time payments and 24/7 availability.

The Hong Kong Monetary Authority (HKMA) is also supporting adoption of FinTech and DLT by collaborating with the Hong Kong Applied Science and Technology Research Institute (ASTRI) to form a FinTech Innovation Hub as well as driving a number of DLT-related initiatives. Hong Kong authorities also seek to better incorporate FinTech and related technologies such as DLT into its regulatory structure. The Security and Futures Commission (SFC), Hong Kong's security regulatory agency, launched a pilot project in late 2016 to use FinTech data to improve its regulatory processes. In addition, a recently launched HKMA Fintech Supervisory Sandbox will facilitate pilot trials of new FinTech products and initiatives that authorised institutions and other FinTech stakeholders can conduct in a live, controlled environment before rolling them out to broader audiences. Finally, HKMA is undertaking research in establishing a central bank-issued digital currency and the use of DLT for secure document validation. HKMA hopes to complete its proof-of-concept on digital currency by the end of 2017. It already has released preliminary results of its research on blockchain and plans to release more information in mid-2018 as it continues its research.

While the level of interest from the regulators is encouraging, the existence of sandboxes as 'safe spaces' for innovation however uncovers the fact that DLT initiatives have not yet found their definite place within the current legal framework and legislative changes will be necessary to provide the financial industry with legal certainty in their activities.

Governance and Cybersecurity Challenges and Controls

Information Integrity

DLT provides a superior ability to preserve information integrity. In order to change any past information after the participant consensus has been reached, information in all subsequent blocks would have to be changed as well, at a huge computational expense and with the changes visible to all the participants, making information in the blockchain practically immutable. Strong information integrity protection is the only inherent and clear security-related benefit of DLT over traditional technologies.

However, while the core DLT is proven to be resilient to information integrity attacks, integrity could be still compromised in case of a client software (wallet) compromise and this will be discussed further down.

Privacy and Confidentiality

Privacy in DLT refers to the ability for network participants to control which information stored in the DLT is exposed to other network participants. According to the DLT design all network participants have access to the whole ledger and many store their own copies of the whole ledger. In financial services it is to be expected that DLT will contain private protected information as well as information about transactions that normally would not be shared outside of an organisation.

Privacy in DLT is seen as the critical feature for DLT adoption by the industry and for achieving compliance with relevant privacy and data protection regulations.

DLT privacy is additionally complicated by the DLT design which primarily addressed information integrity. DLT is designed to be transparent. The focus on integrity in such a decentralised model requires all the network participants to share information. This transparency is by design, and is critical to maintaining trust: every participant verifies every transaction. Bottom line is that anything recorded onto a DLT can be arbitrarily inspected without any restrictions by all participants.

Nonetheless, measures can be taken to enhance privacy. Addressing information confidentiality and privacy in DLT can be achieved through number of controls complementary, rather than inherent to DLT, such as encryption or data anonymisation.

In addition to addressing the confidentiality of protected information stored in the DLT it is important to consider the confidentiality of meta-data stored in DLT. In addition to transactions being stored transparently; public keys that transact are anonymous but fixed meaning that transactions and transaction participants can be easily tracked over time. Applying advanced analytics approaches to that data could also lead to de-identification of participants and creation of new sensitive data.

To further exacerbate the problem, many jurisdictions are implementing the “right to be forgotten” laws providing consumers an option to request their personal information to be removed from the databases. If information needs to be removed from a DLT it might be challenging to implement due to the immutability of DLT as well as its distributed nature. In an implementation in which many counterparties have copies of the DLT it would be difficult to prove that all data has been deleted.

Smart contracts are autonomously executed software programs stored in DLT and used to automate business processes on DLT. In order to execute the coded logic, smart contracts require access to the data stored in DLT and that creates additional risk of leaking confidential consumer data as well as confidential business information.

Practices and controls to consider

<u>Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), and Data Protection Impact Assessment (DPIA)</u>

From the previous paragraphs it follows that DLT adoption may entail a high risk to the privacy of the persons whose data are processed as well as to the confidentiality of business data that might be stored in DLT.

Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), and Data Protection Impact Assessment (DPIA) processes are conducted at early stages of DLT projects to understand if, and to what extent the DLT solution will have privacy and data protection impacts. Such an assessment leads to further insight into the data protection aspects of the envisioned DLT application and it also offers a useful point of reference to help ensure privacy and data protection compliance. It will increase the likelihood that privacy and data protection requirements are embedded into projects at the outset which may also prevent excessive privacy compliance costs later down the road.

Encryption

In a traditional system each party had a wide variety of controls and technologies at their disposal to secure the data at rest or at transit according to their policies. In DLT majority of the ability to control access to data is centralised in the encryption. DLT requires an even stringent focus on encryption than traditional controls with a particular focus on key management. Another related control to consider is encrypting the ledger with more than one key and applying on-chain encryption. Encryption is the critical control and will be elaborated further down in the paper.

Sharding

The original DLT design requires from the each node to store all states state (account balances, contract code and storage, etc.) and process all transactions. Sharding is an approach where the space of possible accounts is split into a number of subspaces (shards) and each shard gets its own set of validators. Transactions within the same shard would work in the same way as they work in the original design, but additional complexity might be introduced in order to achieve data sharing between the shards. Sharding can help with privacy and data protection challenges directly as well as indirectly by improving, although not guaranteeing, anonymity against behavioural profiling and metadata correlation.

Pruning

Another approach to reducing the amount of data stored in distributed ledgers is using pruning (deleting) of old blocks based on the security, performance and/or regulatory requirements. By reducing the amount of historical data available for correlation the process could improve anonymity against behavioural profiling and metadata correlation.

Multiple Key Pairs

Creating fresh key pairs for each new transaction is another privacy-preserving strategy that can further frustrate metadata correlation efforts.

Controlled Key Mapping

In a majority of financial services DLT use cases there is a need to be able to map keys to network partcipants. In such cases a centralised authority may be established to keep the mapping between keys and entities and protect the identity of network partcipants.

Centralisation

Centralisation is an approach in which a DLT is contained only within one, or few, strictly controlled locations in order to localise the information and reduce exposure. In this approach participants simply message transaction requests to these central authorities and receive certain crypto-based proof of successful transactions. Privacy and confidentiality is improved since majority of the participants don’t have access to full ledger, however, this approach undermines the key positive features of DLT and offer no, or very limited, advantage over well-established approaches based on databases and messaging platforms.

Tokenisation

In addition to on-chain encryption, there are other approaches to anonymise the data stored on the DLT. One of those is tokenisation in which each participant replaces the sensitive information it owns with a unique token and it manages its own mapping between sensitive data elements and tokens.

Zero-Knowledge Proof (ZKP)

ZKP are new approaches attempting to produce a perfectly anonymous and confidential cryptocurrency system. Approaches are still experimental, but it is an area of research to be followed and potentially adopted for other DLT uses.

Decentralised Nature

One of the primary differences of the DLT technology compared to the traditional is hinted in its name. Traditional centralised model of data storage and sharing can ease implementation and management of security controls that are focused on the technology they are trying to protect. DLT shifts data storage and data sharing from the centralised model to a decentralised and dynamic model in which every DLT network participant has access to all the data and intended levels of security has to be achieved through new and innovative security approaches.

Key Management

As with any crypto-based infrastructure, and potentially even more, protecting keys is paramount to ensuring the security of a DLT. DLT implementations rely on the cryptographically generated public and private keys to operate. Main challenge associated with cryptography is that stringent policies and procedures must be followed when managing keys, including people, processes and technology.

DLT combines the message and the asset in a single record. Once an asset is embedded into a distributed ledger, possessing the associated cryptographic keys is the only way to retrieve or move the asset. By contrast, in a traditional IT model, a key protects the database, which in turn protects the data or the asset. When the key and the asset are the one, anyone who obtains the key can exploit the asset instantly and there are no additional controls to overcome.

While the DLT technology itself has proven itself to be tamper-resistant, the most impactful vulnerabilities end up being those related to key management and to the application layer key management solutions – the wallets holding the keys. Private keys are the direct means of authorising activities from an account, which in the event they get accessed by an adversary, will compromise any wallets or assets secured by these keys. The protection of the keys is mission-critical.

The methodology of the attacks seeking to gain unauthorised access to a system via stolen credentials remains fundamentally the same-try to capture information, plant malware and/or use social engineering to steal the private keys from the user's machine.

Potentially different private keys could be used for signing and encrypting messages across the distributed ledger. An attacker who obtained encryption keys to a dataset would be able to read the underlying data. However, if the signing key is secured, they will not be able to modify the data or interact with that smart contract.

The significance of protecting the private key is due to the fact that actions taking place on a hacker's machine, such as file decryption attempts or private key reproduction, are not subject to server imposed query limits and are run without anyone else being able to notice.

Unlike with traditional systems, where before a server administrator was capable of tracking attempts to break into a customer or user account, the malicious users can keep trying limitlessly to decrypt or try to reproduce a private key out of encrypted data from a given ledger. With DLT, there is no way of knowing this is happening until after the hacker has succeeded.

Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of the mechanisms and protocols associated with the keys, and the protection afforded the keys. Cryptography can be rendered ineffective by the use of weak products, inappropriate algorithm pairing, poor physical security, and the use of weak protocols. All keys need to be protected against unauthorised substitution and modification. Secret and private keys need to be protected against unauthorised disclosure. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys.

Practices and controls to consider

HSM

Hardware security modules (HSMs) are the technology solution to safeguard and manage digital keys. A successful DLT systems needs highly reliable methods of interfacing with the strong key protection practices afforded by HSMs. Moving the cryptographic functions from software to dedicated hardware devices reduces the risk of processor errors. 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, HSMs increase operational efficiency. To mount a successful attack, attackers either need to have administrative privileges, access to data before it is encrypted, or physical access to the HSM(s).

Multiple Signatures

Use rules that require the use of multiple signatures to authorise and/or create transactions

Recovery Agents

Allow the use of recovery agents-one way of doing this is through a trusted third party which holds, the keying material required to recover keys

Different Keys

Use different keys to sign and encrypt

Signing Governance

Enable internal identification of the individual signing off the request for a transaction

Individual Keys

Issue individual keys to persons working on behalf of institution allowing audit and supporting investigations.

Consensus Hijack

In decentralised, permissionless networks, where consensus is formed through majority, taking control of a large enough portion of participating clients could allow an attacker to tamper the validation process. This is often called the “51% attack” – When more than half the computing power on a DLT mining network is controlled by an entity, it can effectively collude to certify false transactions by being able to produce new blocks faster than the rest of the network (in proportion to their computing power) leading participants to consider that chain as valid.

The extent of a consensus hijack will allow an attacker to refuse to process certain transactions as well as to re-use an asset which has already been spent.

Another consequence of such an attack is in the perspective of adoption. Any chain coming under attack might see an outflow of participants, leading to the question of which chain should be considered as the “main” one to follow as well as potentially crippling the value of that chain.

Another challenge comes from consensus protocols that do not involve some way of penalty to the participants. In this way for a malicious user would be easier to attack.

Practices and controls to consider

Limit Node Processing Ability

Make it difficult for a node to process a large number of transactions.

Processing Power Monitoring

Monitor if one of the nodes increases processing power and is executing a significantly higher number of transactions.

Anomaly Detection

Consider advanced analytics approaches to monitor for participants' anomalous behaviour.

Sidechains

Sidechains extend DLT functionality by implementing multiple interoperable distributed ledger networks. Sidechains, due to their nature of being more specialised and typically having a smaller number of network participants are more at risk of a consensus hijack attack.

They are also introducing additional risks to the whole network of DLTs when sidechains participate in transfer of assets and messages between chains. In those scenarios sidechains might introduce a fraudulent transaction into the parent chain after a sidechain has been compromised.

Practices and controls to consider

Merged Mining

Require the use of merged mining, where the proof of work applied to validate the parent chain may also be used to submit valid blocks for the sidechain.

Exploited Permissioned DLT

Just like a traditional approach where databases are controlled by a centralised authority, permissioned DLT networks where consensus is controlled by a central authority are at risk of the central authority being exploited. Just like in the traditional systems, the key risks to be addressed are unauthorised or fraudulent actives by the central authority – whether due to a malicious insider or due to capabilities being hijacked.

Practices and controls to consider

Background Checks

Implement usual practices to manage risks and monitor for malicious insiders.

Authorisation

Implement traditional controls for authorising and monitoring privileged activities.

Processing power monitoring

Monitor if one of the nodes increases processing power and is executing a significantly higher number of transactions.

DDoS

Distributed nature of DLT introduces an additional risk of any of the participant intentionally, or inadvertently, consuming too much of the DLT processing resources and impacting the service. For example, if a rouge member starts pushing a large volume of irrelevant transactions, the network processing to validate the transactions, checking for fraudulent transactions, etc. could grind the network to the halt.

Practices and controls to consider

Block Noisy Participants

Monitor the network for "noisy" participants. In case of a permissioned DLT, it would be possible to ignore or block such a participant.

Writer Nodes Restriction

Depending on the use case, a potential approach could be to restrict which nodes can offer new transactions for validation. While all the nodes in the network would have a read access, only carefully vetted and secured nodes could introduce new transactions. Attempts by other nodes to introduce new transactions could be blocked before too much computing power is expanded on validation.

IP Lock

Similar to the previous solution, in certain cases it might be feasible to accept transactions only from select, authorised IP addresses.

IP/Node Blocking

Infrastructure of the DLT solution should allow admin blocking of IPs/nodes that generate too many new transactions. This could be manual, or automatic based on certain thresholds.

New Transaction Fees

Depending on the use case, the system could assign fees to be charged for every new transaction request. Such approach would make it difficult for a node to issue a large numbers of transactions.

Security and Privacy of Clients

Wallet management represents the process and technology used with which a wallet software operates with the keys assigned to it. The wallet software would need to protect the keys from being accessed without authorisation, in both cases while stored, but also while in operation with the software.

Practices and controls to consider

Make sure the software for the wallet does not leave the key accessible in plain text outside the application.

Require the implementation of recovery keys.

Smart Contract Management

Smart contract management refers to the people, processes and technology used when creating a smart contract. Smart contracts are essentially programs that run on the distributed ledger. They are prone to any faults associated with code. As with any software, the more complex a smart contract is, the more prone to software errors it will be.

Practices and controls to consider

Code Review

Smart contracts are codified in DLT using an applicable scripting/programming language. Consider implementing usual software security best practices such as code reviews. A party, independent from the development team, with a similar skillset, should review all of the smart contract code before it is pushed into production.

Functions Standardisation

Consider standardising regular functions into libraries and protecting them against unauthorised modifications through strong change control. Limiting the parameters and bands that could be used for key functions through such standardisation would reduce opportunities for introduction of malicious code.

Smart Contracts Library

Next level of protection could be achieved by developing and standardising a library of carefully vetted and approved smart contracts.

Scalability

Practices and controls to consider

Sharding

The original DLT design requires from the each node to store all states state (account balances, contract code and storage, etc.) and process all transactions. This provides a large amount of security, but greatly limits scalability: a DLT can only process as many transactions as a single node can. In large part because of this, current public implementations such as Bitcoin or Ethereum are limited to a small number of transactions per second. Sharding is an approach where the space of possible accounts is split into a number of subspaces (shards) and each shard gets its own set of validators. As long as there are sufficiently many nodes verifying each transaction that the system is still highly secure, but sufficiently few that the system can process many transactions in parallel and therefore greatly improve DLT throughput.

Pruning

Pruning concept, available in certain implementations of DLT, allow for historic transactions to be pruned without peer coordination. The feature is facilitated via pruning predicate functions, provided along any smart contracts a given system is desired to host. For certain use cases pruning of historic transactions from blockchain systems could yield significantly reduced storage requirements for some categories of applications, especially such with low transaction interdependency.

Mini-blockchain

For certain DLT use cases, the concept of mini-blockchain might address the scalability issues. The mini-blockchain introduces the “account tree”, which is basically a balance sheet storing the balance of every account. With this change, transactions do not need to be stored forever in the DLT. Only the most recent transactions and the current account tree have to be stored. The mini-blockchain is thus much more scalable than the original blockchain since the mini-blockchain only grows when new accounts are created.

The mini-blockchain consists of 3 components:

1. Account tree
2. Transaction tree
3. Proof chain

First, the account tree is a Merkle tree of all the accounts in a given block, each account being a data block with an address and a balance (it can have more data fields, if necessary). Second, the transaction tree is a Merkle tree of all transactions in a given block, each transaction representing a change to a number of accounts. Third, the proof chain is simply a chain of blocks where each block contains a nonce, the top hash of the account tree and of the transaction for that block and the hash of the previous block. Basically, it is the headers of a normal blockchain.

Quantum Computing

Quantum computing may threaten the premise of asymmetric cryptography. Popular security algorithms that are used for securing information through a complicated challenge (e.g. RSA, ElGamal), may now be resolved in a shorter amounts of time through the use of quantum computing. Though quantum computing does not seem to represent an immediate threat, it should be certainly taken into consideration for a future-proof solution.

Practices and controls to consider

Post-quantum Cryptography

Post-quantum cryptography refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer. It is an area of active research with a growing number of quantum secure cryptographic systems and encryption schemes being developed.

Conclusion

The modern financial services industry has evolved to include a range of complex network of participants and processes with firms on every side of a transaction depending on an overlay of controls to be sure that everything is done right. DLT is now making it possible to rethink which relationships make sense, and whether they are still necessary. The disruptive potential of eliminating financial market intermediates – combined with the ability to streamline network and transaction costs, free up capital and reduce market and regulatory risk – allows unprecedented business opportunities in financial services.

If DLT is to gain wide acceptance in financial services, promoters should acknowledge and address the concerns. DLT is new, but it has matured rapidly. The controls are different, but they can be designed and managed. Technical expertise is rare, but it can be found, especially in those organisations that have made a commitment to the technology. DLT is now being firmly embraced by many of the most respected institutions in the world. For the DLT to move from proof-of-concept stage to commercialisation and broader acceptance, security and privacy concerns have to be addressed. PwC believes that we are now at the tipping point and there are real, practical, cost effective solutions for blockchain assurance.

We expect that blockchain assurance will include the following steps:

- Evaluating the business use case and the needs of all stakeholders.

- Assessing the underlying cryptography, including how private keys are managed and how DLT security is maintained. This would include reviewing the consensus mechanism being used to be clear about when a new record should be added.

- Examining how the specific network has been set up, how that system's reports are being generated, and the controls that guide that network's operation. Keep in mind that there is no such thing as a standard DLT. There are many DLT systems, and each implementation is unique.

- Performing ongoing reviews to assess the effects of any systemic changes.

Using the approach described here, defusing concerns about distributed ledgers is now within reach.

Annex F

Innovative Application of Law to Facilitate DLT

Disclaimer
The information provided in this section is for general reference only.
It does not constitute legal advice and should not be treated as such.

For a complete and definitive statement of law, direct reference should be made to the relevant legislation(s). The Law Society of Hong Kong makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information herein. Legal advice should be sought independently if the reader has any questions about any legal matter.

The Law Society will not be liable, either express or implied, for any errors in, omissions from, or misstatements or misrepresentations of information contained in this section, and will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage however arising from or in respect of any use or misuse of or reliance on the information contained in this section.

Author
Technology Committee
The Law Society of Hong Kong

Data protection

1. Accuracy, retention, rights to be forgotten and disclosure

General

The concept of Distributed Ledger Technology ("DLT") is to enable parties to enter into transactions with each other without an intermediary in a trusted way. The perpetual and open nature of data in DLT is one way to ensure security and trustworthiness in transactions.

Insofar as privacy issues relating to DLT are concerned, there is the question of whether, as a general principle, it is better not to store personal data in the DLT but only a pointer (and hash) to a traditional database so that personal data can be purged (and its integrity checked) when necessary. It would seem that, taking the example of smart contracts using DLT, even if personal data in DLT can be masked and only a pointer is contained, unless certain technologies are applied, the entire sequence of actions taken in a smart contract are propagated across the network and/or recorded on the blockchain, and therefore are publicly visible. Examples of such technologies include Hawk and Corda. Hawk is a compiler developed to create a cryptographic protocol between users, the manager, and the blockchain to preserve on-chain privacy. Corda, another DLT platform, also contains some mechanisms to protect privacy.

Although it may be better not to store personal data in DLT in order to avoid risks of violation of privacy laws in disclosure, it would seem that even if personal data in DLT are stored in a pointer and hash, that may still be caught by privacy laws if the transactional details publicly available can enable the ascertainment of the individuals in the transactions concerned.

On the other hand, a totally permissioned system (i.e. a private, dedicated network) for transactions by DLT could also offer privacy and confidentiality protection to such transactions.

At the moment, it seems premature to arrive at a conclusive view as to whether or not the replacement by pointer/hash of personal data is a way that personal data privacy can be protected, and in any event, whether that is the only way for personal data privacy protection.

Purpose limitation

Data Protection Principle ("DPP") 1 under the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") says that personal data must be collected (and therefore accessed) for a purpose directly related to a function/activity of the data user. This raises the question on whether a node holding personal data that would be assessable by other node complies with the DPP. The answer to this will depend on whether the nodes hold the data on behalf of others (validation and authenticity-checking for others) or use such data for its own purpose (to create and complete a transaction).

It is worth noting the example of internet service providers ("ISPs") which are generally not viewed as "data users" (under the definition at section 2(12) of the PDPO) when personal data uploaded by their subscribers are circulated on the internet. The data users are, in that case, the subscribers, not the ISPs, which merely transmits data on behalf of another and not for any of its own purposes.

Using same analogy, if a node (Node A) needs to hold the personal data merely because it has to assist other nodes in data validation or authenticity checking, there may be an argument that Node A is not a data user. In any event, the data subject should be informed about how DLT stores its data. Saving the hashed (or encrypted) personal data on DLT may also serve Node A's purpose if just used for calculation.

Data accuracy

While the data stored using DLT would always carry the hash values which cannot be amended, the right to rectify inaccurate data is possible as the same can be appended to the DLT chain. Accordingly, it seems the risk of violation of data accuracy principle for data stored in DLT would be low, although further research may be necessary.

Data retention

The data stored using DLT would always carry the hash values which cannot be amended and that is a way to ensure trustworthiness of the transactions, as those hash values would need to be preserved in order to ensure security and the ability to verify authenticity of the transactional data.

The data retention policy requires that all practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

As explained above, it is possible for “personal data” to be removed from the data stored using DLT using various measures, such as by replacing them with pointer/hash values. In this case, the risk of violation of personal data privacy laws should be mitigated.

It is also possible for the data stored in DLT to be within a private network rather than a public network. It is in this case that the issue of whether or not personal data stored in such private DLT may be violating the data retention principle. However, the issue here is on “necessity” of the retention of the data — if the personal data is contained in order to verify the authenticity of the data concerned, would that qualify as being “necessary” for such personal data to be retained? Would it be appropriate to compare the same with conveyancing transactions — would the storage and the requirement for verification of all historical deeds of transactions constitute violation of personal data privacy laws?

Rights to be forgotten

The European Court of Justice decision on the rights to be forgotten only applies to publicly available data. This risk could be mitigated so long as the relevant data stored using DLT are private in nature; or alternatively, if data stored using DLT is public in nature, with all personal identifiers removed. Currently, Hong Kong does not have such rights to be forgotten.

Data access and correction

DPP 6 under the PDPO provides a data subject the right to access and correct his/her personal data held by data user. Given the nature of DLT, every block in it is made unalterable. If a data subject wishes to correct the data, a new block can be created and this correction block must be chained with the original block. Although it seems unsatisfactory that the original incorrect block cannot be deleted, a suggestion is that the data subject should be informed that the correction block will never be detached from the chain in this case.

2. Cross-border data flow/data localisation

Given some of the restrictions on cross-border personal data flow or requirements on data localisation, the storing of personal data outside of the DLT may be a solution that allows more flexibility for data users/controllers to comply with such requirements.

For example, the new Cybersecurity Law of the PRC will require all important data and personal information of “critical information infrastructure” to be stored within Mainland PRC. Storing of personal data outside the DLT would make it easier to comply with this rule (subject to the determination as to whether the data constitute “important data”).

The EU does not allow cross-border data flow except if the other jurisdiction has a similar level of protection of personal data. If however the data transferred in the DLT do not contain personal data, it may be easier for such data or DLT to comply with the EU cross-border data flow requirements.

Transfer of data outside Hong Kong will be governed by section 33 of the PDPO which is not yet in force. Under section 33(2) of the PDPO, there is a list of scenarios where transfer is acceptable. The most practical method is to obtain the data subject's consent in writing prior to the transfer (section 33(2)(c) of the PDPO). Another method is to have consensus (or agreement) between all nodes on the level of protection of data privacy required (at least with the same standard as in Hong Kong).

Furthermore, the use of permissioned DLT (i.e. DLT in a private network) may also sufficiently address cross-border data flow and data localisation requirements. It is because the organisation could control the flow of the data using permissioned DLT, by requiring that those without the necessary permission and/or outside the relevant jurisdiction are not able to decrypt the data stored within the DLT structure.

3. Access by law enforcement agencies

A lot of tensions have been created in the area of personal data access by law enforcement agencies. The storing of personal data off the DLT can be a simple solution so that such personal data cannot be arbitrarily accessed by any node (including foreign entity) without the right legal basis and oversight, but sometimes it is inevitable to transfer and access personal data in DLT.

There is also the issue of accessing and using personal data stored in the DLT without the consent of data subject, if personal data is stored in the DLT which is then accessible by all nodes of the DLT. Some problems and observations are set out below.

4. Universal solutions

Regarding the data protection issues of accuracy, retention, right to be forgotten, cross-border data flow and data localisation, there is the question of whether there can be a universal solution to these issues or whether each of these regulatory requirements is so different that they require different solutions separately. If personal data would be stored on DLT, two things should be worked on in parallel: (1) on one hand, the DLT should fully explain to the data subject in a Personal Information Collection Statement ("PICS") the scope of and extent to which their data will be collected, used, transferred, stored and retained, and seek their written consent and confirmation if possible; (2) on the other hand, discussion and negotiation with cross-border nodes about all applicable data privacy protection laws and policies should take place, then an agreement and guidance prepared for all nodes to sign and comply with. This may be achievable in a permissioned DLT but for an unpermissioned DLT, where the identity and jurisdiction of every node may not be fixed and known, storage of personal data off DLT may be a better option.

5. Traditional databases

In the case of personal data being stored in a traditional database, Hong Kong law requires that data users must observe the six DPPs, which are set out in the PDPO, while handling personal data of data subjects, specifically in the collection, use, processing, storage, erasure and security of personal data.

Non-compliance with the DPPs does not constitute a criminal offence directly. Upon breach of any DPPs, the Privacy Commissioner may serve an Enforcement Notice to direct the data user to remedy the contravention and/or instigate the prosecution action. Contravention of an Enforcement Notice constitutes an offence which could result in a maximum fine of HK$50,000 and imprisonment for two (2) years.

The six DPPs are as follows:

DPP1: Collection of personal data

DDP1 concerns the purpose and manner for which the personal data is collected. It provides that personal data must be collected in a lawful and fair way, for a purpose directly related to a function and activity of the data user. By way of example, a company collecting job applicants' personal data by means of recruitment activities, when in fact it is not really recruiting anyone, is an example of unfair means of personal data collection. Further, data subjects must be notified of the purpose of collection, and the classes of persons to whom the data may be transferred. Only adequate, but not excessive, personal data is to be collected in relation to the purpose.

In order to inform the data subject of the purpose of collection, companies usually provide PICS to data subjects on or before the collection of personal data to inform data subjects about what data is to be collected/used/processed, and for what purposes.

DPP2: Accuracy and retention of personal data

DPP2 stipulates that all reasonably practicable steps must be taken by the data user to ensure personal data is accurate and is not kept longer than is necessary to fulfil the purpose for which it is or is to be used. In cases where data processors are engaged, data users also have to prevent any personal data which is transferred to the data processor from being kept longer than necessary by the data processors.

DPP3: Use of personal data

DPP3 provides that, unless the data subject has given prior voluntary and explicit consent for use for a new purpose, personal data shall only be used for the purpose for which the data is collected or for a directly related purpose.

Data users must always state the purposes for which the data is collected and may only use the data for the said purposes. If any personal data collected is to be used in a way not envisaged before, an assessment needs to be carried out to ascertain if the new purpose/use is directly related to the said purpose of data collection. If not, consent from data subjects must be obtained before using the data.

DPP4: Security of personal data

According to DPP4, data users need to take all reasonably practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use having regards to the harm that could result.

Data users must always ensure that the transmission and storage of personal data are protected by measures such as encryption, password protection and access control based on "least-privileged rights" and "need-to-know" principles.

DPP5: Disposal of personal data

DDP5 provides that data users should formulate and make available to data subjects policies and practices in relation to the handling of personal data (including the types of personal data and the collection purposes).

Data users can, for example, make sure a Privacy Policy Statement is readily accessible on the internet and which contains specific coverage as to how data stored would be handled.

DPP6: Access and correction of personal data

DDP6 provides that data subjects should be able to access any personal data about themselves which is held, and should also be able to correct such personal data.

Industry-specific personal data protection

In addition to the PDPO, certain types of information may be protected by specific rules and regulations. For example, the collection, sharing, use, and safe keeping of patients' health data that is stored in the Electronic Health Sharing System (the "System") (a system that provides an information infrastructure platform for healthcare providers in both the public and private sectors) would be governed by the Electronic Health Record Sharing System Ordinance (Cap. 625). With consent of the patient, healthcare providers can have access to and share a patient's health record in the System for healthcare-related purposes.

6. Consent requirement

Under the PDPO, data subjects' prior consent is of the utmost importance concerning the life cycle of a piece of personal data.

Before the collection of personal data, individuals must be provided with a channel, at no charge, through which they can indicate whether or not they consent to the use of their personal data for a prescribed purpose, e.g. for direct marketing. Further, before any personal data is used, e.g. for direct marketing purposes or for any purpose other than the purpose for which the data was to be used at the time of the collection, data users (e.g. businesses) must obtain prior consent from data subjects.

Unauthorised use of personal data, e.g. disclosure of personal data without consent with an intent to either make a financial or other gain or cause financial loss or other property loss to the individual, is an offence. Unauthorised disclosure of personal data obtained from a data user without the data user's consent and which causes psychological harm to the data subject, irrespective of intent, also constitutes an offence. This happens, for example, where a member of hospital staff obtains medical records of a patient, discloses them to someone else without the hospital's consent, and the disclosure causes the patient psychological harm. These offences can attract a fine of up to HK$1 million and five (5) years' imprisonment.

The PDPO allows a few exemptions to the above requirements, including an exemption for national security interests and exemptions for matters such as disclosures to law enforcement officials and processing data in connection with legal proceedings.

7. Legal implications arising from cryptographic or consensus algorithms breaks

Most DLT implementations today are based on traditional cryptosystems and consensus systems. For example, most digital signature schemes used on DLTs are the Elliptic Curve Digital Signature Scheme. Elliptic Curve Cryptosystems ("ECC") were invented by Neal Koblitz and Victor Miller in 1985, and the Elliptic Curve Digital Signature Algorithm is the elliptic curve analogue of the Digital Signature Algorithm proposed in 1992 by Scott Vanstone, which was accepted in 1998 as an ISO standard (ISO 14888-3) and accepted in 1999 as an ANSI standard (ANSI X9.62) for digital signatures[1].

In August 2015, the US National Security Agency ("NSA") had warned that ECC is not a long-term solution of cryptography. The NSA suggested that there is a need to develop post-quantum cryptography, and encouraged the development of the same[2]. Despite these researches, it appears there have been arguments that what the NSA suggested was not true, and ECC remains a secure form of cryptography[3].

[1] Don Johnson, Alfred Menezes and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", accessible at http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf

[2] Neal Koblitz and Alfred J. Menezes, "A Riddle Wrapped in an Enigma", in IEEE Security and Privacy, accessible at https://pdfs.semanticscholar.org/cb7c/0bb16f37904c42cbc3805aa0438ea3d98864.pdf

[3] Ditto.

Legal implications in Hong Kong

There is a lack of research on potential legal liabilities in the event that cryptographic algorithms are broken and security of information contained in DLTs are compromised, leading to loss suffered by parties on the DLTs. Traditional tort law focuses on causation — whether the loss suffered by the claimant was caused by the defendant's wrongdoing, and whether it satisfies the "but for" test, i.e. is it correct that the claimant would not have suffered the damage but for the defendant's wrongdoing? The law recognises the doctrine of remoteness of damage, i.e. whether or not the claimant's loss was reasonably foreseeable. In *Wagon Mound (No. 2)* [1967] 1 A.C. 617, the Privy Council held the defendant liable in tort on the basis that there was some foreseeability of the kind of damage, namely fire, however remote the possibility may have been[4].

Applying the traditional rules of tort to the breaking of cryptographic algorithms, the question would be whether the loss suffered by the breaking of the cryptographic algorithms: (1) was caused by the relevant defendant, for example, be it the relevant financial institution which adopted the algorithm, or the relevant security service provider who provided the security protection solution; and (2) was it reasonably foreseeable to the person who allegedly committed the tort, which was not in law too remote a consequence of the defendant's wrongdoing? It would be an exercise to determine whether the relevant defendant knew or should have known that there is a risk of breaking of the fundamental cryptographic algorithms of some DLTs, i.e. whether the financial institution has been adopting a cryptographic algorithm which is known to contain security risks, and whether or not there was any viable alternative to prevent the loss. If the relevant cryptographic algorithm is widely recognised to be secure, with no evidence to suggest that the algorithm could be easily broken by hackers, and no evidence to suggest that the relevant defendant has failed to implement sufficient technical measures, it would be unlikely that tortious liability could be attributed to the defendant concerned.

Where there is a contract, the above principles still apply but the terms of the contract will also be looked at in determining the key factors regarding potential liability; save for the terms of a contract, the damages would be such as to put the claimant in the same position as if the contract had been performed. Where a person is not a party to the contract then the Contracts (Rights of Third Parties) Ordinance (Cap 623) may apply to provide rights where the same have not been excluded by the contract. Where there are services, then the Supply of Services Implied Terms Ordinance (Cap 457) would apply. Leaving aside those liabilities that cannot be excluded under law, limitation and exclusion of liability terms within a contract could limit and restrict applicable rights and losses, provided the said clauses are reasonable and the court is most likely to interpret the clause based on business common sense.

Exemption clauses

As to whether or not one could include an exemption clause exempting liability for any loss caused by the breaking of a cryptographic algorithm, pursuant to section 7 of the Control of Exemption Clauses Ordinance (Cap 71), no exemption clause may exclude or restrict one's liability for death or personal injury resulting from negligence and, for any other loss or damage, one cannot so exclude or restrict his liability for negligence except in so far as the term or notice satisfies the requirement of reasonableness. Pursuant to section 3 of the Control of Exemption Clauses Ordinance, the requirement of reasonableness is satisfied only if the term was a fair and reasonable one to be included having regard to the circumstances which were, or ought reasonably to have been, known to or in the contemplation of the parties when the contract was made, and whether the term or notice expressed is a language understood by the person as against whom another person seeks to rely upon the term or notice.

[4] See, Clerk and Lindsell on Torts, 19th Edition, paragraph 2-121

It is noted that there have been multiple reports recently on incidents of bitcoin wallet thefts[5]. Causes of these thefts include insufficient measures imposed by the wallet operators, or negligence of the users (e.g. having a password which is not secure enough, or failing to securely keep the hardware token), or fraud of the particular wallet operators. In-depth research needs to be conducted as to the precise causes of these bitcoin wallet thefts, and for regulators to consider publishing guidelines and/or licensing requirements to operators on preventive measures for the breaking of DLTs in general. It is noted that the Securities and Futures Commission has recently published a consultation paper on proposals to reduce and mitigate hacking risks associated with internet trading[6], and Hong Kong regulatory authorities might well consider whether a consultation should be conducted on security risks prevention of DLTs and adoption of certain international standards for the implementation of DLTs by banking and financial institutions, for example.

Legal implications in other jurisdictions

Where the DLT extends to multiple jurisdictions which may or may not follow the English common law system, the laws in each of those countries relating to each of the key factors would have to be considered. Given the rapid change of technology and innovation in applications, any dispute will fall to be determined by the factors at the time of the negligent act and within the legal jurisdiction concerned, if it can be ascertained. To avoid uncertainty and reduce risk, one available option would seem to be the adoption of a choice of law clause with a possible arbitration clause for the determination of disputes. In disciplines where technology, applications and obligations undergo rapid change, a court would, looking at a situation retrospectively, find it difficult to assess the tortfeasor’s obligation in prospect, for an innovation would not then have come to fruition nor invented or discovered. The answer may lie in the adoption of policies which are able to keep up with the fast pace of change and implemented in segments of time. Such polices could cover security and other obligations as and when they become common knowledge.

By way of example, the Elliptic Curve Digital Signature Scheme is deemed to be one of the best technological signature systems available at present (notwithstanding the comments set out above regarding the ECC) and, for the purposes of liability, it would need to be assessed from the stage of knowledge presently available. Quantum crypto analysis is presently a ‘known unknown’, that is, unknown as to its effectiveness in breaking cryptographic or consensus algorithms. It is possible that the law of negligence may develop along the lines similar to claims formulated under the concept of ‘loss of chance’ based on the probability of the harm. What then of the ‘unknown unknown’, that is, innovations that no one has as invented or discovered, but could be invented or discovered? Surely the harm must then be viewed from the knowledge of the tortfeasor as they would be the only person capable of knowing the damage that could be caused. Civil law only provides remedies where there are pre-existing relationships and obligations but perhaps statutory protection would be required to provide remedies in civil claims, and where harm extends to the public at large then criminal sanctions should be considered. Clearly, given the multinational issues, there is a need for establishment of international treaties which could be ratified by signatory states.

[5] See, for example, http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP and https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#d6591f238bad

[6] See http://www.sfc.hk/edistributionWeb/gateway/EN/consultation/doc?refNo=17CP4

The law might have to be introduced to apportion liability where the connection between the person and the end result would become disconnected by intervening person or systems that are automated. Product liability would reside in the developer of the software and hardware systems.

With the increase in the use of DLT and eventual government support of DLT infrastructure, it will inevitably lead to the development of a local and international digital identity merged with, for example, mobile phones.

Cross border

8. Cross-border DLT

If a DLT is used across different jurisdictions, it would currently have to be dealt with in the traditional way of dealing with multi-jurisdictional contracts, unless and until unified rules can be agreed between users/ parties, the DLT industry and/or states regarding cross-border DLT.

For example, parties are free to agree on the applicable law and, in the absence of an agreement on the choice of law, any relevant law, directive, convention or common law rules may be applied to determine the governing law of the DLT verification/ transaction (which may be treated as a regular contract or, in common law jurisdictions, as giving rise to a duty of care under the common law of tort). Given the decentralised nature of DLT, and as with multi-jurisdictional contracts, this means that there may be more than one applicable law and each party would likely argue for the applicable law that is most favourable to it. The same also applies in determining the applicable jurisdiction for resolution of DLT disputes (to the extent that it has not been agreed between the parties).

In terms of liability and legal enforceability, it may be difficult to identify where a breach or fraud has occurred in a decentralised system and who may be ultimately liable (e.g. the current DLT user, a previous DLT user, one or more decentralised autonomous organisations ("**DAOs**"), a DAO creator, or other related parties). There is an added level of complexity in bringing a claim against DAOs given their undefined legal status. Other potential issues include identifying the correct defendant, its location and assets. As a result, and as with multi-jurisdictional contracts, even where liability is determined in accordance with applicable laws, it may still be difficult or impossible to enforce the contract or any legal award subsequently obtained.

The above issues will also be applicable in terms of discovery and extra-territorial reach.

9. Potential universal solutions

As with multi-jurisdictional contracts, there are different ways of dealing with the various legal issues arising; agreements may be reached between individual DLT users, the DLT industry generally or even between states.

For example, when setting up a new blockchain, the system could generally require all parties to agree on certain legal issues, such as applicable law and dispute resolution forum, before they can use the relevant DLT (either as part of the terms and conditions to use the DLT or as a separate contract or framework agreement between the parties) in order to reduce uncertainty.

Alternatively, the blockchain industry could develop:

(a) a universally recognised set of commercial terms or definitions that could be used by any blockchain party (e.g. the International Commercial Terms/INCOTERMS published by the International Chamber of Commerce, which sets out defined terms and their meanings to establish certain roles, risk allocation and liabilities between parties that can be used in commercial contracts involving the transportation of goods); or

(b) a set of binding rules that individual blockchain parties could sign up to (e.g. see the EU Binding Corporate Rules in relation to cross-border transfers of personal data).

A universal solution could also lie at state-level. For example, states could agree on, or sign up to, unified international directives, rules, treaties or principles regarding DLT which would apply in all cross-border situations. Such unified directives/rules etc. could:

(a) be recognised only by those states that choose to ratify the rule (see, for example, the Hague Choice of Court Convention (relating to applicable law); or the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (relating to dispute resolution)); or

(b) require member states to enact local laws to implement the relevant rule, giving member states some leeway in applying the international rules (as per the traditional method in which EU law applies to EU member states); or

(c) be made automatically binding on (i) users and DAOs within all member states; and even (ii) users outside of member states who offer goods or services to those within member states (see, for example, the broad and general binding nature of the EU's General Data Protection Regulation).

However, it is unlikely that all users and relevant parties will be able to agree on a universal solution for all of the legal issues discussed above (i.e. applicable law, legal enforceability, liability, dispute resolution, discovery and extra-territorial reach), so the development of DLT over time may well lead to different solutions for different issues.

10. Principle of geo-fencing on DLT transactions and legal implications of physical data repository

With the development of platforms which, by design extend beyond physical and jurisdictional borders, the concept of 'geo' in terms of physical geography has, indeed since the advent of the world wide web, ceased to exist in reality and moved to a concept. The concept should be 'virtual jurisdictional boundaries'.

The principle of geo-fencing can be applied in respect of a DLT if the geographical area of a data inputter, user, device or transaction can be identified and tracked, for example, by using an IP address, the Global Positioning System ("GPS"), Radio Frequency Identification ("RFID") or other means of location identifiers. Geo-fencing can be used to better enable and/or to restrict DLT applications.

For example, in cross-border trade finance applications, geo-fencing can be used to: identify the location of a transaction or party; identify use of an application or software in a particular location; restrict transactions to users or transactions in certain geographical areas; or as a means of authenticating a particular user or transaction.

Applying geo-fencing to on-chain transactions would mean that location data is in the main chain of a DLT and available to all nodes of that DLT; in an unpermissioned network such data would, therefore, be publicly accessible.

In applying geo-fencing to off-chain transactions only, the location data is not in the main chain of the DLT and therefore it may be difficult to ascertain the location of a node or data user etc. at the material time. However, geo-fencing could be applied for off-chain use in authentication or know-your-client ("KYC") procedures, for example, where the use of on-chain geo-fencing might not be acceptable due to concerns in personal data being publicly recorded in a DLT. We have discussed above some of the issues relating to personal data in the DLT.

If all data are encrypted in a DLT, although this may help to protect location/personal data and to address privacy concerns, legal considerations would need to be given as to who would (or should) have access to any passwords or keys necessary to decrypt the data. An inability to access or review unencrypted data may contradict the open nature of data that is central to DLT, and may raise issues in identifying correct users or transactions etc. There is also the question of what encryption standards would be adopted in the DLT, and who would be liable in the event that the encryption standards used did not adequately protect data.

In addition, there may be legal concerns if encrypted data are stored at some foreign states physically, raising the issue of whether foreign states or regulators would be able to access (or require access to) encrypted data. This issue would apply equally to any unencrypted data recorded in a permissioned DLT that is physically stored in a foreign state.

Legal basis

11. Use of digital assets and documents — Considerations prior to deployment of DLT

Blockchain revolutionises the value of 'trust', which is a necessary element of a transaction or relationship. That 'element' being the key to the value of trust. This is the key to identification of the asset. Thus if the identity of a person along with all information as to that personal identification is the value required then trust in that identity is the asset. The personal identification has value for various purposes for verification by sellers or service providers. For verification by a buyer, it is important to note the identity of the seller and the person to whom the payment is to be made. Identity of a legal person is the primary asset for many transactions related to person-to-person transactions. This information is permanent and unchangeable without record. Other issues such as the right to confidentiality and the right to be forgotten, for example, if that asset relates to certain identification documents or personal identifiers such as identity card, then data privacy laws must be taken into account. The requirement of compliance with laws as to restriction or standards could best be achieved through pre-identification/verification of assets rather than encryption restrictions which is in compliance with the democratisation of trust in a distributed system as opposed to a centralised system.

12. Digitising an original document for the DLT to ensure the digitised version(s) have the same legal standing as the original document

Regarding digitising an original document for the DLT, the general law/practice/procedure applies regardless of it in the context of DLT or otherwise. Generally speaking, a digitised version can never receive the same legal standing as its original non-digitised version, but it is more a matter of admissibility/weight as evidence in the course of court proceedings.

13. Settlement finality

This area of the law is unknown in the Hong Kong jurisdiction. In the EU, there have been different schools of thought in the last 3 years but not a settled one.

14. Legal responsibilities of physical asset custodians relative to DLT operators in case of off-chain assets represented as on-chain digital assets

Introduction

Blockchain technology offers a superior level of security over traditional client-server databases, due to the distribution of data over a set of servers/nodes. This advantage is achieved by tamper-proofing data with a proof of work protocol produced by a timestampted hash that chains previous entries to the database. The above process results in a set of data that cannot be retroactively changed unless the attacker manages to achieve control of over 51% of nodes connected to the network[7]. The implementation of blockchain has been successfully demonstrated by the Bitcoin cryptocurrency, which was the first to utilise this protocol. Expanding beyond the mere realm of databases, novel applications that utilise blockchain technology continue to find ways to decentralise current businesses and industrial practices. One major technology that added considerable value to the blockchain ecosystem is the Ethereum protocol which allows users to deploy Decentralised Application ("**Dapps**") on the blockchain. Dapps are operated by smart contracts which regulate the way the application behaves given that certain variables are presented for computation[8]. Smart contracts can be used to create automated DAO entities which run independently of any human control on the Ethereum blockchain[9].

Given the considerable benefits that blockchain offers in the safe transfer of value, it is possible for this technology to be used to assist in the record maintenance of physical assets. Currently many types of assets are deposited with custodians that provide storage and security services, the most common are precious metals that are stored in highly secured vaults. A certificate evidencing the value stored in the vault is issued to the owners which can be exchanged or redeemed. Technologies such as Ethereum enable the creation of blockchain tokens that can be used as a substitute for a certificate of deposit for a physical asset. An example of such service is the DigixDAO Dapp that uses Ethereum smart contracts to create and distribute blockchain tokens that represent bullion gold[10].

Structure of the Token

Blockchain tokens may seek to emulate certificates of deposit function in a manner similar to any other cryptocurrency. The token itself uses asymmetric cryptography, also known as Public Key Infrastructure ("PKI"), where the public key is represented as an address on the blockchain and the private key gives the user the ability to make a record on the blockchain with the given address[11]. As the private key allows the holder to write changes on the network, security of the private key is of significant importance.

Legal Responsibility on the Parties in the Scheme

The relationship between the custodian and the token issuer is subject to private agreement(s). The primary legal responsibility of the custodian would be that of a bailee, where the possession of the physical asset will not grant the custodian any rights and titles to the physical asset[12]. Due to this relationship, the custodian will be under a duty of care to preserve

[7] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' <www.bitcoin.org> page 3

[8] Vitalik Buterin, 'Ethereum White Paper: A next generation smart contract & decentralised application platform' page 34

[9] Eric Vollstadt, 'What are Dapps?' (*Bitnation*, March 16, 2015) <https://blog.bitnation.co/what-are-dapps/> accessed 28/04/2017

[10] Anthony C Eufemio, Kai C Ching and Shaung Djie, *Digix's Whitepaper: The Gold Standard in Crypto-Assets* (2016) page 5, Figure iii

[11] Nakamoto at page 6

[12] Dr Nathan Tamblyn, *Chitty on Contracts - Hong Kong Specific Contracts* (Fifth edn, Sweet & Maxwell), chapter 3 para 3,002 citing *The Owners of Pioneer Container* [1994] C.L.C 332

the value of the physical asset[13], additionally as the relationship is governed by a private agreement the burden to prove the bailment relationship will not need to be put into dispute as the custodian will have full knowledge of his duties[14]. The custodian would likely not be liable beyond his relationship with the token issuer and the duty to deliver the assets to the lawful owner of the assets. The duties of the custodian will not terminate upon the cessation of contractual dealings between the custodian and the issuer[15] until the assets are returned to their lawful owners.

The relationship between the issuer of the token and the token holder would be governed by the terms and conditions of the token issue. The legal right to the physical asset can remain with the issuer and the beneficial ownership would attach to the token. The nature of responsibility of each party to such scheme will greatly depend on the structure of the token service[16]. As mentioned above, DigixDAO issues tokens for bullion gold on the Ethereum network, however the structure of DigixDAO is autonomous. DigixDAO deploys smart contracts that issue tokens representing gold to holders. This process is accomplished by creating an asset card[17] for the gold stored in the vault by the custodian where audited information about the gold is recorded on the blockchain ("Asset Cards"). These Asset Cards are then sent to a smart contract that will mint tokens in return for the Asset Cards. In order to redeem the gold, the token has to be converted to an Asset Card by using a smart contract which can be presented to custodian for redemption. In this type of scheme, DigixDAO assumes liability for the representation that in fact the gold is contained within the designated vault, and the issuer would need to make arrangements to properly audit any holdings to give sufficient assurances to the token holder that the assets are actually present in the given vault, such as DigixDAO which documents extensively their auditing policy and allows for inspection of Asset Cards on the blockchain.

The liability of the token holder relates to being able to securely store the private key. Due to the novelty of such services, tokenised physical assets may not enjoy any deposit insurance protection, as participation in such schemes is voluntary. One may apply *caveat emptor* as a default principle of responsibility of the token holder.

Liability for losses

In the event of loss, the degree of liability will depend on the causation of the loss in question. As discussed above, the custodian would be liable for any breaches of his duty. In the DigixDAO example, the gold vault operator (the custodian in this scheme) would be liable if the vault security was compromised and would need to ensure redemption is made to the lawful owner of the asset on the Asset Card (further details on redemption are discussed below).

[13] Ibid at para 3,019 citing *Wong Tung Fuk v Tang Wing Sze Irene* [2013] HKLRD 627

[14] Ibid at para 3,023

[15] Ibid at para 3,024 citing *The Sea Empire* [1992] 1 HKC 357

[16] An example of such smart contract can be found in the following link <https://github.com/DigixGlobal/digixdao-contracts/blob/master/contracts/Token.sol>

[17] The technical process for the creation is described in DigixDAO white paper

A considerable degree of liability would be imposed on the issuer of the token, the degree of exposure of the issuer liability will depend on the structure of the scheme and the private agreements between the issuer and the token holders. The more centralised the control of the issue of the token, the greater the potential liability of the issuer. In the DigixDAO scheme, the issue of tokens is made by smart contracts and such operation are done autonomously beyond the control of the DigixDAO entity. In this type of scheme, liability will depend on the technical integrity of the smart contract code, many DAO style projects implement a policy of transparency by clearly documenting their technology and open sourcing their code for public audit and inspection.

The liability on the token holder arises out of the level of security that the Token Holder operates to protect his private key. The private key is essential to produce transactions on the blockchain and the token holder has full responsibility for the security of the private key, which can be accomplished by using further encryption, password access or an external device for enhanced protection. In some circumstances losing the private key can result in the complete loss of access to the tokens stored, although recovery systems such as a mnemonic or physical recovery device may be used to regain access. Legal protection only offers some retroactive measures such as criminal prosecution of hackers under computer crimes legislation in Hong Kong[18], but this is conditioned on the law enforcement's ability to sufficiently track down the aforesaid hacker. Token holders who lack sufficient expertise in digital security may elect to entrust their private keys with a depository or key manager that may provide the security on their behalf but in doing so the token holder would create another bailment relationship.

The disadvantage of this type of service is that should it become large enough to attract the attention of potential cyberattack campaigns, the private key may be susceptible to loss.

Redemption of Physical Assets

As discussed above the token holder would need to present tokens for Asset Cards to the custodian for the redemption of the physical asset. The custodian has the duty to ensure delivery of physical assets to the true owner of the asset in order to avoid conversion[19]. The procedures for redemption would be regulated by the private agreement between the custodian and the token issuer and such agreement should contain sufficient measures to ensure redemption is made by the rightful owner of the token. Hypothetically the custodian may allow redemption by a simple presentation of the decrypted PKI signature of the token by the token holder[20]. Such a simple process is susceptible to unlawful redemptions as criminals can simply use stolen private keys to make redemptions, thereby creating a higher level of liability on the custodian. In order to mitigate this risk, the custodian may deploy proactive and reactive measures to facilitate a safer redemption process. For example, proactive measures include requiring further forms of verification of the private key owner, such as verifying other data that are associated with the public key, presenting transaction history or requiring the original physical device that contains the private key. Reactive measures can include the collection of KYC documentation such as national identity card/driver's license/passport information, proof of address etc. Such measures may also be necessary in order to comply with relevant anti-money laundering and counter terrorist financing legislation. While there is no perfect solution, token issuers and custodians can implement a variety of verification mechanisms that will mitigate the risks.

[18] Unlike the UK, Hong Kong does not consolidate computer related offences under one statue, please refer to Benson Tsoi, *Archbold Hong Kong Criminal law Pleading Evidence & Practice* (2017 edn, Sweet & Maxwell 2017) Chapter 43, for a complete list of computer crimes in various Hong Kong Ordinances.

[19] *Halsbury's Laws of Hong Kong - Banking and Finance*, vol 40 (LexisNexis Butterworths), para 40.197 citing *United States of America and Republic of France; v. Dollfus Mieg et cie. S.A. and Bank of England* [1951] AC 582

[20] Such procedures would be ill advised as the custodian possess a high level of liability for wrongful delivery, as stated in [1951] AC 582.

Blockchain backed tokenised physical assets will most likely become a popular way to trade the rights to assets, and such technology can benefit precious and industrial metals markets where the metals are always kept in safety vaults or warehouses for a considerable period of time before the owner redeems them. Such schemes would likely be regulated by private agreements and policies of the custodians and token issuer who will regulate by design of the architecture of the token itself. As both the custodian and the issuer will likely disclaim any liability in the case of losing the private key, the token holder has the ultimate responsibility to keep its token credentials secure. Regulators may in the future impose higher standards for verification with regard to redemption procedures if public policy dictates that such standards are necessary although free market incentive may possibly generate technology to provide sufficient safeguards to token holders. As blockchain physical asset backed tokens are still in a period of infancy, there is considerable room for further research and development to develop more robust token systems. It is likely that a token issuer who invests in a secure and transparent architecture will become the favoured by the general consumer.

Anti-money laundering

15. Anonymous DLT in financial services or transactions

Given the primary requirement of KYC in the proper management of risk in AML/CTF legislation, personal identification is a key element of the value of trust. The proper method of alignment to this value would be unpermissioned DLT provided the key element of personal identification can be guaranteed, if not, which is unlikely, a permissioned DLT should be considered.

16. Liabilities and redress for programming or smart contract errors

Code is law/Smart contract

Definitional background

A "smart contract" is a colloquialism, and is neither legally defined by law nor a technical term. Smart contracts generally have two components: the "contractware" and the "DLT." They contain immutable coding to promote transactional certainty *ex ante*. The "contractware" part of the smart contract program automates execution and exercise human discretion from performance. The contractware is self-interpreting and self-enforcing: it processes/interprets factual input and delivers the intended output; and it has control over, at least some of, the physical and/or digital objects needed for performance. The DLT builds in an external neutral self-help mechanism for smart contract parties. A smart contract is meant to be self-contained and obviates enforcement by judicial or arbitral intervention. "Strong" smart contracts allow for no or little room for revocation and modification (by the parties or enforcing courts/tribunals), and vice versa for "weak" ones. In this sense, "strong" smart contracts also provide no or little room for non-performance.

There was a recent DAO attack in June 2016 on "Ethereum" and DAO , the smart contract that sat on it. As Cheng Lim and TJ Saw stated:

"The DAO was a smart contract intended to pool investment funds (which, at one point, totalled $150M worth of the cryptocurrency 'Ether') which could be allocated by members of the DAO to different projects. A hacker spotted a mistake in the programming of the smart contract, and utilised it to drain the Ether from the DAO into child DAOs controlled by the hacker. Importantly, the underlying Ethereum blockchain and smart contract both functioned in the pre-determined way in which they were designed, but the failure of proper smart contract design created a functional vulnerability which ultimately undermined the intent of the DAO."

Liabilities & Redress

It depends on how the loss-causing behaviour arose – is it at the point of the DLT, DAO, or other support software or online environment? Various factual issues need to be addressed. For example, are there particular problematic codes programmed into the DLT and how foreseeable were they in causing the type of damage that arose? Was the underlying software used in ways that were typically expected of users? Who manages the various systems involved in operating the DLT? It may be problematic making a claim in a decentralised contract network due to evidentiary hurdles given the emphasis on anonymity.

There might be redress against the creator of the loss-causing codes in the same way as claims have been litigated against developers and distributors of defective software under various legal claims, including breach of contractual warranties (or related consumer and trade laws, under the heads of merchantability and fitness for a particular purpose) and tortious theories. Three tort theories of product liability are potentially applicable: negligence, malpractice (e.g. where licensed professionals are involved) and strict product liability. The usual elements must be proved (e.g. the developer must owe a duty of care to the user). Under all three tort theories, a plaintiff can recover damages associated with (a) the loss of valuable data (e.g. data can be valuable due to security classification or regulated privacy); (b) destruction of raw materials; and (c) destruction or loss of property other than the product itself.

17. Programming bugs in smart contracts

Given the fast development of the technology and the law surrounding DLT and smart contracts, it helps to contextualise the matter with analogies. For example, vending machines are contractware, as defined above. If they worked as intended, soda cans should be dispensed upon inserting the correct amount of cash without human intervention. Sometimes they erroneously withhold the soda cans and the change, and sometimes they dispense more than they should. The consumer usually has no way to find out how exactly the machine works before entering the transaction. And, the company operating the machines usually have a complaints hotline to resolve problematic transactions including refunds etc. The questions about the binding nature of the transaction, rights to recourse and loss remediation could be answered in comparable ways between those relating to vending machines and smart contracts in financial markets. With these factors in mind, we consider the issue of programming bugs in smart contracts below.

(a) It depends factually on how the underlying computer codes and the nature of the "bugs" themselves. Also, it depends on whether the smart contract included modification, reformation, termination, and rescission clauses, and how their representation in code impacts on execution, performance and enforcement.

Each smart contract is a self-contained system with self-interpreting and self-enforcing functions, and the roles and functions of the underlying codes matter in the legal characterisation. If both parties never intended to have the relevant codes included and/or executed, the remedies associated with mutual mistake and *non est factum* might be available to render the contract voidable or unwind the transaction.

In most cases, smart contracts would be standard contracts, for example, as part of a larger exchange, and the relevant codes would be part of the design but they could lead to "unintended" consequences. In such cases, there might still be a binding contract but there might be lawful remedies depending on the nature of the terms breached and the severity of the breach. Damages might arise depending on the remoteness of the loss.

(b) It depends on, again, the nature of the bugs and how the bugs were exploited. A third party might be liable under third party interference of a contract or guilty of a crime under a number of statutes. Under the Crimes Ordinance, ss. 59 and 60 extend respectively the meaning of property to include any program or data held in a computer or in computer storage medium, and the meaning of criminal damage to property to misuse of a computer program or data. Under the Crimes Ordinance, s. 161 sets out the offence of access to a computer with intent to commit an offence or with a dishonest intent. Similarly, s. 27A of the Telecommunications Ordinance sets out the offence of obtaining unauthorised access to any computer by telecommunications. The Theft Ordinance, s. 19 extends the meaning of false accounting to include destroying, defacing, concealing or falsifying records kept by a computer. Similarly, s. 85 of the Crimes Ordinance extends the meaning of making false entry in a bank book to falsification of the books of account kept at any bank in electronic means.

(c) Legal liabilities might be found within the framework of the smart contract or the legal arrangements associated with the transaction. Under contractual and tortious principles, the party causing the loss would be responsible, and any party contributing to the loss would have contributory liability. So, the main issue is whether causation can be proven under the relevant case theory and whether there is any contributory negligence. There could be, for example, a claim against a party inducing the transaction, a third party hacker, the exchange operator (if human-operated), the creator of the smart contract, and any broker or advisor involved.

(d) Restitution, rescission and other legal remedies to reverse the transaction causing the loss might be available if a contractual or tortious claim were made out, depending on the facts (as discussed above). The relevant laws should be consulted on this point.

(e) By design, most operative parts of smart contracts are immutable once executed. The contract terms might be hardwired on an exchange or DAO, and their immutability is indeed a trait enticing investors to transact on smart contracts. Where software patching is available in the system, it might be justified to prevent further losses. The remediation probably has no effect on the losses already incurred and the associated legal liability.

18. Components required to constitute a legally binding smart contract

With reference to the definition above, a “smart contract” has the effect of a contract, but it takes on many forms. It should not be understood as a contractual document in digital form. Referring to the vending machine example, the main legal relationship exists between the consumer and the soda can vendor and not with the machine, which is a distribution agent. This relationship includes but also exists beyond the machine. The smart contract usually contains the mechanics for execution, performance and enforcement, but it might not contain the entirety of terms forming the contract at law.

The relevant question therefore is what sort of legal remedies are sought and under what claims. If a party desires to seek contractual remedies and enforce the smart contract as a contract at law, then the common law contract requirements would need to be proven to have existed contemporaneously during the purported contractual relationship between the relevant parties. The requisite elements that must be established to demonstrate the formation of a legally binding contract are: (1) offer; (2) acceptance; (3) consideration; (4) mutuality of obligation; (5) competency and capacity; and, in certain circumstances, (6) a written instrument.

It is also noteworthy that commonly a user enters into a transaction involving smart contracts by a click-wrap agreement (and there is case law in Hong Kong and overseas providing guidance on click-wrap agreements). The user, however, is agreeing to the terms of the click wrap agreement, which might or might not incorporate the terms of the smart contract (it could be simply the service terms for access a trading portal).

There may, however, be other ways to characterise the smart contract and its relationships with the relevant stakeholders, which could give rise to legal recourse. This might be founded on a legal binding contract, such as securities trading on exchange or DAO, or some other grounds, such as negligence, restitution and fiduciary duty. The remedy of unjust enrichment might be available in the case of the restitution of unjust gains resulting from a breach of a smart contract. Such a remedy is often associated with mistakes of fact or law, total failure of consideration, duress and undue influence. Under what condition would smart contracts be subject to securities regulation is beyond our current scope, however.

Given the underlying risks of modelling errors and complex contract interdependencies, the performance of each smart contract carries the risk of failing to reflect the intentions of its creators. As such, it is recommended that smart contracts should be adopted only if their design follows the latest best practices and international standards. The smart contract community is developing boilerplate codes to be embedded as safeguards but there is no legal requirement for their use. For example, integrating "escape hatches" or clean paths for modifying and undoing contracts in light of unforeseen eventualities (the DAO lacked this feature entirely), which would allow human intervention under strict conditions (e.g., all party approval), without realistically threatening the immutability of smart contracts. By contrast, contracts at law have "escape hatches", including modification, reformation, termination and rescission clauses, but they also have the added advantage of post-agreement malleability which smart contracts lack. Escape hatches of smart contracts must be developed at the creation stage – at the library, platform, cryptocurrency levels etc. It would be useful to have international, transnational and/or domestic regulation sanctioning such requirements.

Mortgage related

19. Issues relating to documents required to be "in writing" (e.g. deeds and conveyances relating to land)

Under the Electronic Transaction Ordinance ("ETO") (Cap. 553), Schedule 1 explicitly excludes any deeds, conveyances or other documents or instruments in writing, judgments, and lis pendens referred to in the Land Registration Ordinance (Cap. 128). This means that the documents set out in Schedule 1 of the ETO cannot be electronically signed. In addition, the Property Conveyance Ordinance (Cap. 219) specifically states that related documents should be signed, sealed and delivered, which raises the question of whether this means that these documents must be in written form in order to be legally binding. We look at some of these issues below.

State/Governmental Blockchain Issues

Given the vast efficiency benefits offers by blockchain technology many governmental and public organisations have commenced research into possible blockchain solution for public services. The previous Financial Secretary, John Tsang, included a blockchain agenda as part of his budget speech[21]. When discussing the application of blockchain technologies the government, one key distinction that needs to be raised is the fact that government is naturally a centralised institution. This means the blockchain nodes may not be openly public

[21] Government of HKSAR, 'The 2016 Budget - Fintech' (2016) <http://www.budget.gov.hk/2016/eng/budget11.html> at para 63

and the government may wish to control the proof of work on the blockchain. There are consortium blockchain solutions on the market which only grant node access to a select few, such a Hyperledger and R3, which hypothetically makes it possible for the government to run a blockchain as a consortium with nodes being distributed amongst different governmental departments or going further by allowing the legislative and judicial functions of the State to provide certain oversight to operation of nodes as a means of propagating checks and balances in a state administered blockchain. The security strength of a blockchain depends on the number of unaffiliated nodes that support the network, therefore consortium blockchains may possess deficient security features as the affiliation amongst nodes can be directed by a central authority that may maliciously, recklessly or negligently tamper with information on the blockchain[22].

The blockchain provides the ability for verification of the information stored as each entry is timestampted with a unique hash and the nodes have to determine by consensus if the information is valid. If executed correctly public blockchains can create highly secured and reliable public registries. Hypothetically every governmental register can utilise the benefits from the blockchain, one example is the Land Registry. Although e-conveyancing has been a controversial subject in the past and has not been implemented fully in any Anglo-Saxon common law jurisdiction, blockchain technology can support e-conveyancing systems as a database backend and it can support traditional paper based registry system as a more secure alternative to a client-server database.

Issues with e-conveyancing

E-conveyancing issues predate blockchain technology as the topic has been a subject of debate for a number of years in various jurisdictions. Procedures for conveyancing of land are highly formalised and have to made in accordance with various statutory requirements going as far back as the 17th century Statute of Frauds in England and Wales[23]. One of the key requirements for any land transaction to be valid is that it has to be made in writing. In Hong Kong, s.3 of the Property and Conveyancing Ordinance requires the land contract to be in writing (or, if made orally, reduced to a written memorandum) and signed[24]. All deeds disposing land must also be written, signed, sealed and delivered. These statutory requirements raise questions of whether a digital or source code version of a land contract and deed can be classified as a writing and what can be classified as a signature for the purposes of the Property and Conveyancing Ordinance[25].

The first issue of writing under Hong Kong law does not seem as optimistic as perhaps in other jurisdiction that recognise computer generated contracts as “writings”. Schedule 1 of the Electronic Transaction Ordinance excludes contracts for the sale of land and deeds for the deposition of land. This specific exclusion indicates that the policy makers where not inclined to allow for electronic versions of conveyancing documents to be used as part of the land transfer process. A second issue of signature requirements have been raised in other jurisdictions where the debate has centred around the most appropriate form for a digital signature.

In consideration of the above analysis, a blockchain land transfer system powered by computer generated land contracts and deeds is not possible under the current legal regime in Hong Kong. A blockchain alternative to the Land Registry database may be implemented as a means of enhancing security of land registry data.

[22] Vitalik Buterin, ‘On Public and Private Blockchains’ (*Ethereum Blog*, August 7th, 2015) <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> accessed 28/04/2017

[23] Statute of Frauds 1667

[24] SH Goo and Alice Lee, *Land Law in Hong Kong* (Third edn, LexisNexis Butterworths 2010) page 70

[25] Ibid page 80

European developments in e-conveyancing

Development in e-conveyancing systems in the European Union have been more progressive than in Hong Kong. The controlling legislation with regard to this matter is the European Electronic Signatures Directive which adopted the UNCITRAL Model Law on Electronic Commerce and Model Law on Electronic Signatures. The Directive recognises three kinds of electronic signatures[26]; the first being a simple signature embedded on a website such as a "I Agree" button or the signatory's name on an e-mail; the second being an Advanced Electronic Signature ("**AES**") which by definition resembles a conventional PKI cryptographic signatures; and third, a Qualified Electronic Signature ("**QES**") which is a AES accompanied by a certificate issued by designated authority[27].

The use of QES signatures have become more widely used with countries such as Sweden, Lithuania and Estonia integrating QES signatures within the national ID program, allowing citizens to use a highly secured QES as part of an e-Government strategy[28]. Estonia and Lithuania have begun research on implementing an e-conveyancing system that will use the abovementioned QES signatures.

State-run blockchain applications would require a much more different approach than those in the open market, due to the centralised nature of governmental operations. Nonetheless the technology can provide the State with the same benefits as in the open market. However, in order to successfully implement such a solution more research and development efforts will be required to find an optimal implementation for a State blockchain.

If such a solution is successfully implemented, many State registers can be reallocated on the blockchain, however a change in policy and legislation may be needed to implement blockchain for certain registers such as the Land Registry.

Due to the strict formalities in land conveyancing procedures, currently it is not possible in Hong Kong to conduct e-conveyancing as the legislation which legitimises computer-generated contracts specifically excludes any contract for the sale and deposition of land. DLT could be used as a database for Land Registry records however a full utilisation of DLT to conduct conveyancing is currently not possible until the policy makers see fits to reform the existing legislative framework to allow for e-conveyancing to take place.

Trade finance related

20. Electronic shipping documents

At present, a ship-owner, charterer and their agents issue bills of lading signed by the master of the vessel upon receipt and loading of goods on to a vessel. Simple digitisation of that form with the relevant particulars and signature by a digital signature would not affect the legal validity of a bill of lading as this has already been incorporated in practice by many shipping companies.

21. The transparency along the trade chain and sharing of information on DLT

The transparency along the trade chain is improved by stakeholders sharing information on DLT, such as the production status by the seller, and the shipment status by the freight forwarder/shipping company. The transparency nature of information stored in blockchain to its participants raises the question of whether the sharing of all trade finance information to all parties may be a legal issue (e.g., is it necessary to have "opt-in" and "opt-out" procedures for the ecosystem stakeholders to agree on the extent of information to be shared, and to specify the special conditions to opt out information sharing? Can this simply be dealt with by terms and conditions of use?).

[26] Seamus Keating, 'Digital Signatures and the Electronic Transfer of Land' (2013) 7 Masaryk University Journal of Law and Technology 49 page 52

[27] Ibid page 53

[28] Ibid page 58

In Hong Kong, the Electronic Transactions Ordinance (ETO) does not exclude the use of electronic shipping documents, but it does exclude the use of negotiable instruments in electronic form (apart from cheques that bear the words “not negotiable”), as well as any instrument the making, execution or making and execution of which is required to be stamped or endorsed under the Stamp Duty Ordinance (Cap 117) (other than a contract note to which an agreement under section 5A of the Stamp Duty Ordinance relates). Furthermore, it would be impossible for any contracts or documents signed by or with any government entity or any person acting on behalf of a government entity to adopt DLT, since the definition of “digital signature” under the ETO requires certification by a “recognised certificate” issued by those certification authorities recognised by the Government Chief Information Officer.

Accordingly, the crucial issue with implementation of DLT in trade finance lies in acceptance of the same by different players and parties in trade finance, including customs of different countries/regions, freight forwarders, banks, insurers, and all other agents involved. Our ETO may need to be updated to expressly recognise DLT as a form of recognised digital signature, in order that transfer of an electronic shipping document from one party to another on the DLT can be recognised to represent ownership title transfer of physical assets.

Provided that all the relevant players in international trade finance accept electronic shipping documents on DLT as proof of title, and our ETO is properly updated to facilitate the same, it does not seem that the sharing of all trade finance information to all parties would be an issue, as such information would unlikely be information relating to a living individual and the Personal Data (Privacy) Ordinance and privacy laws of other jurisdictions would unlikely be relevant.

It is further noted that the sharing of accurate information on DLT may also assist in the prevention of fraud and money laundering in international trade finance activities.

There have been reports that IBM and Maersk were working together to digitise, manage, and track shipping transactions using blockchain technology[29]. In addition, the Department of Justice of Hong Kong SAR Government will be been participating in the United Nations Commission on International Trade Law relating to the topic of modernising international trade law to support innovation and sustainable development[30]. The adoption of DLT in international trade is a topic highly relevant to the harmonisation and modernisation of the laws and rules of international trade and commerce which is being considered at UNCITRAL, and research and collaborations may be further conducted to foster development in this regard.

[29] See, for example, http://www.reuters.com/article/us-usa-blockchain-ibm-idUSKBN16D26Q

[30] See, for example, the participation by the DOJ in the UNCITRAL 15th Session Congress in Vienna on 3-20 July 2017, at A/CN.9/XL/INF/2

Digital-ID related

22. The legal requirements for the collection, use, retention, security and disposal of Hong Kong Identity Card ("HKID") and HKID number

According to section 4 of the PDPO, "*[a] data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under this Ordinance.*"

The following are paragraphs from the *Code of Practice on The Identity Card Number and Other Personal Identifiers* issued by the Privacy Commissioner for Personal Data (April 2016) that seeks to give practical effect to the 6 DPPs under Schedule 1 of the PDPO:

(a) *Data Principle 1 – purpose and manner of collection of personal data:* no data user may compulsorily require an individual to furnish his HKID number.

(b) A data user should not collect the HKID number of an individual except in the following situations:

- pursuant to a statutory provision which confers on the data user the power or imposes on the data user the obligation to require the furnishing of or to collect the HKID number; or

- for the following purposes: (i) as the means for the future identification of the holder of the HKID Card where such holder is allowed access to premises or use of equipment which the holder is not otherwise entitled to, in circumstances where the monitoring of the activities of the holder after gaining such access or use is not practicable; or (ii) as a condition for giving the holder of the HKID Card custody or control of property belonging to another person, not being property of no value or of a value which is trivial in the circumstances.

Data Principle 2 – accuracy and duration of retention of personal data

(a) A data user should not collect from an individual his HKID number except by:

- means of the physical production of the HKID in person by the individual;

- accepting the number as shown on a copy of the HKID which the individual chooses to provide rather than present his HKID in person; or

- first accepting the number as furnished, and later checking its accuracy and authenticity by means of the physical production of the HKID in person by the holder, or if that is not reasonably practicable, by means of a copy of the HKID provided by the holder, before the number is used for any purpose.

(b) The data user should take all reasonably practicable steps to erase the record of a HKID number upon the holder of the HKID leaving the premises or ceasing to have the use of the equipment concerned (as the case may be), or within a reasonable time thereafter.

(c) The data user should take all reasonably practicable steps to erase the record of a HKID number upon the holder of the HKID ceasing to have custody or control of the property concerned, or within a reasonable time thereafter.

Data Principle 3 – use of personal data

A data user who has collected the HKID number of an individual should not use it for any purpose except:

- for the purpose for which it was collected;
- for linking, retrieving or otherwise processing records held by it relating to the individual;
- for linking, retrieving or otherwise processing records relating to the individual held by it and another data user where the personal data comprised in those records has been collected by the respective data users for one particular purpose shared by both; or
- for a purpose to which the holder of the HKID has given his prescribed consent.

Data Principle 4 – security of personal data

(a) A data user should take all reasonably practicable steps to ensure that a HKID number and the name of the holder are not:

- displayed together publicly; and
- made visible or otherwise accessible together to any person, other than a person who needs to carry out activities related to the permitted uses of the HKID number.

(b) A data user should not issue to an individual any card (not being a HKID or driving licence) bearing in a legible form the HKID number of that individual, including such number in its original or an altered form from which it is reasonably practicable to deduce the HKID number.

(c) A data user shall take all reasonably practicable steps to ensure the security of any system it controls for assigning a personal identifier to an individual. Such steps shall include all reasonably practicable measures to safeguard against the unauthorised assignment of the personal identifier to an individual and to prevent the unauthorised production of the identification documents, if any, it issues bearing the personal identifier that it assigns to the individual.

Data Principle 5 – information to be generally available

All practicable steps shall be taken to ensure that a person can:

- ascertain a data user's policies and practices in relation to personal data;
- be informed of the kind of personal data held by a data user; and
- be informed of the main purposes for which personal data held by a data user is or is to be used.

Data Principle 6 – access to personal data

A data subject shall be entitled to:

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data: (i) within a reasonable time; (ii) at a fee, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

23. Privacy policies of a Digital-ID system

If a Digital ID system is developed to have an interface with the general public for them to interact directly (e.g. to enter identity-related information), we consider below some points which the privacy policy should include and how it should be written.

What should the privacy policy include?

(a) *Collection of data* – how data is collected from the general public and how it is used?

(b) *Provision of data* – how general public is invited to provide data, how that data is used and how it is protected?

(c) *Data retention* – how the data is retained, for how long, when and under what circumstances it will be destroyed?

(d) *Disclosure and sharing of data* – data should be confidential but when required, who are the people to which the data is disclosed.

(e) *Transfer of personal data outside Hong Kong* – whether this would happen and how is security of the data safeguarded.

(f) *Security* – how is security for the information is maintained.

(g) *Personal information access and correction* – how data subjects can access their own information and make corrections when required, whether there are charges for such access and correction.

How should the privacy policy be written?

The privacy policy should: (i) be written clearly and easy to understand by general public; (ii) no legalese; and (iii) include in general the following:

- What information is collected;
- Who is collecting that information;
- How the collected information is going to be used;
- If the information is going to be shared with anyone else;
- What choices the customer has about the use and distribution of that information; and
- How a customer can edit or correct the collected information.

Annex G

Blockchain & Liability

Abridgement prepared for the Fintech Facilitation Office of The Hong Kong Monetary Authority of the academic article *Distributed Liability of Distributed Ledgers: The Legal Risk of Blockchain,* available at https://ssrn.com/abstract=3018214

Abstract
The transformative potential of distributed ledger technology, especially in the financial sector, is attracting enormous interest. Many financial institutions are investing heavily in proof of concept demonstrations and the rollout of pilot applications of DLT technology. Part of the attraction of distributed ledger systems, such as Blockchain, lies in transcending law and regulation. From a technological perspective, DLT is generally seen as offering unbreakable security, immutability and unparalleled transparency, so law and regulation are seen as unnecessary. Yet while the law may be dull and the technology exciting, the impact of the law cannot be simply wished away. With data distributed among many ledgers, legal risk will remain. DLT projects may well be found, by courts, to constitute joint ventures with liability spread across all owners and operators of systems serving as distributed ledgers. Regulators seeking to support appropriate approaches to twenty-first century financial infrastructure must focus on these legal consequences.

Keywords: Bitcoin, Blockchain, Distributed Ledger Technology, Financial Infrastructure, FinTech, RegTech.

Authors
Dirk A. Zetzsche
Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg, and Director, Centre for Business and Corporate Law, Heinrich-Heine-University, Düsseldorf, Germany.

Ross P. Buckley
Scientia Professor, King & Wood Mallesons Chair of International Financial Law, and Member, Centre for Law, Markets and Regulation, UNSW Sydney.

Douglas W. Arner
Kerry Holdings Professor in Law, University of Hong Kong.

I. Introduction

Over the past several years, interest in distributed ledger technology (DLT) such as blockchain has exploded[1]. Regulators[2], consultants[3], technology firms[4] and academia[5] are promoting DLT for financial services. Blockchain technology has moved beyond cryptocurrencies, like Bitcoin, and its application is now being considered for all parts of the financial system. Capital raising, trading, clearing and settlement, global payments, deposits and lending, property and casualty claims processing (InsurTech), digital identity management and authentication, and RegTech solutions (such as automated compliance, administration and risk management, and anti-money laundering and client suitability checks) have all been identified as significant potential DLT use cases.

At the same time, legal concerns are emerging. The discussion so far has focused on investment fraud, the classification of crypto-currencies as securities, derivatives, commodities, currency or other assets, systemic risk regulation and central bank functions as well as money laundering and taxation. We seek to add another, private law dimension which has received little attention[6].

While distributed ledgers may well be more secure than traditional centralised ledgers, recent events call for an analysis of who will bear DLT losses and responsibility for damages in connection with a blockchain. Notable examples include the loss of 750,000 customer Bitcoins and 100,000 Bitcoins owned by the Japanese Mt. Gox Bitcoin exchange, the hot wallet hack leading to the loss of 19,000 Bitcoins, valued at about US$5.1 million, by world's second largest Bitcoin exchange Bitstamp, the misappropriation of US$53 million held by the investor-directed DLT-enabled Decentralised Autonomous Organisation (DAO), the loss of 119,756 Bitcoins with a market value at the time of between US$66-72 million by Hong-Kong-based Bitfinex as well as the loss of ETHER worth US$32 million managed by the popular ethereum client called Parity[7].

As these examples show, **risk does not vanish if financial services are provided via distributed ledgers**. In turn it is of the essence to analyse how liability risk formerly concentrated in one ledger is distributed in distributed ledgers.

[1] Focusing on legal and governance issues only: Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 THE CONSUMER FIN. L. Q. REP. 232 (2016); Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191 (2016); Wessel Reijers, Fiachra O'Brolcháin & Paul Haynes, *Governance in Blockchain Technologies & Social Contract Theories*, 1 LEDGER 134 (2016); Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulation Blockchain Transactions*, 65 DUKE L. J. 569 (2015-16); Lewis Rinaudo Cohen & David Contreiras Tyler, *Blockchain's Three Capital Markets Innovations Explained*, INT'L FIN. L. REV. (2016), *available at* http://www.iflr.com/Article/3563116/Blockchains-three-capital-markets-innovations-explained.html; THE LAW SOCIETY OF HONG KONG, INNOVATIVE APPLICATION OF LAW TO FACILITATE DLT (August 2017).

[2] IOSCO, RESEARCH REPORT ON FINANCIAL TECHNOLOGIES (FINTECH) ch. 5 (February 2017), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf; ESMA, REPORT - THE DISTRIBUTED LEDGER TECHNOLOGY APPLIED TO SECURITIES MARKETS (Feb. 7, 2017); Press Release, ASIC, Op-ed: Blockchain, (Oct. 26, 2015) *available at* http://asic.gov.au/about-asic/media-centre/asic-responds/op-ed-blockchain/.

[3] It has been estimated that "distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15-20 billion per annum by 2022": see Santander InnoVentures, OLIVER WYMAN AND ANTHEMIS GROUP, THE FINTECH 2.0 PAPER: REBOOTING FINANCIAL SERVICES (June, 2015), *available at* http://santanderinnoventures.com/fintech2/; WORLD ECONOMIC FORUM (WITH DELOITTE), THE FUTURE OF FINANCIAL INFRASTRUCTURE - AN AMBITIOUS LOOK AT HOW BLOCKCHAIN CAN RESHAPE FINANCIAL SERVICES (2016), *available at* www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf.

[4] *See IBM Blockchain*, IBM, https://www.ibm.com/blockchain/ (last visited July 10, 2017).

[5] Quinn DuPont & Bill Maurer, *Ledgers and Law in the Blockchain*, KING'S REV. June 23rd (2015), *available at* http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/; Eva Micheler & Luke von der Heyde, *Holding, Clearing and Settling Securities through Blockchain/Distributed Ledger Technology: Creating an Efficient System by Empowering Investors*, 11 J. INT'L BANKING & FIN. L. 652 (2016); Philipp Paech, *Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty?*, 21 UNIF. L. REV. 612 (2016).

[6] *Cf*. the underweighted common law dimension of distributed ledgers: Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 WASH. & LEE REV. ONLINE 22 (2014); Max I. Raskin, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 FORDHAM J. CORP. & FIN. L. 970, 970 (2015); Philipp Paech, *The Governance of Blockchain Financial Networks*, MODERN L. REV. 23-34 (forthcoming 2017); from a German civil law perspective: Benjamin Beck & Dominik König, *Bitcoins als Gegenstand von sekundären Leistungspflichten*, 215 ARCHIV FÜR DIE CIVILITISCHE PRAXIS 655 (2015). Very little attention has been paid to the private law sphere in French regulation. However, *see* Press Release, Michel Sapin, Ministre des finances et des comptes publics on *Réguler les monnaies virtuelles* (July 11, 2014), *available at* http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/17768.pdf (stating: "Limiter l'anonymat en imposant une prise d'identité lors de l'ouverture par un professionnel d'un compte en monnaies virtuelles pour un tiers, et en imposant une vérification d'identité pour les retraits et dépôts aux "distributeurs" de bitcoin" – transl. "To limit anonymity by imposing on professionals a duty of establishing identity when opening a virtual currency account for a third party, and by imposing on Bitcoin "distributors" a duty of verification of identity in case of withdrawal").

[7] For details and references *see* Zetzsche, Buckley, Arner, *Distributed Liability of Distributed Ledgers: The Legal Risk of Blockchain*, at I., *available at* https://ssrn.com/abstract=3018214.

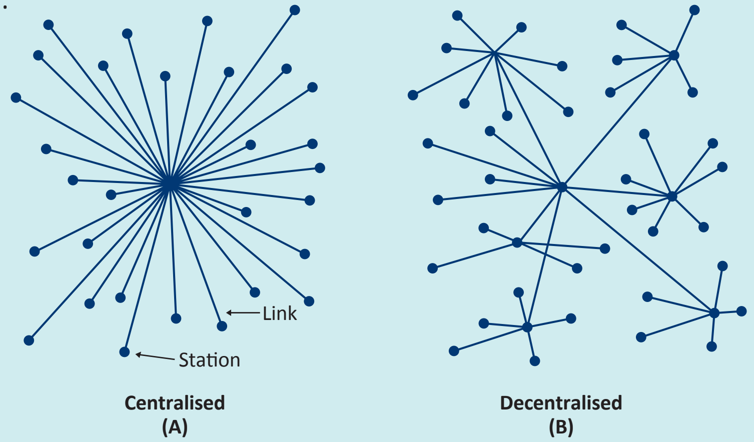
II. Features of Distributed Ledger Technology

A. The Ledger Concept

The modus operandi of distributed ledgers is best understood by looking at their counterpart, the centralised ledger. Centralised ledgers are the most common data storage device in finance today. In a centralised ledger, data are stored on the ledger, and the trusted administrator of the ledger maintains it, recording transfers of assets and the like upon receipt of appropriately verified notifications. Risks exist. The ledger could be destroyed, or more likely, hacked or otherwise compromised, so that the original data are held for ransom or manipulated and replaced by new (inaccurate) data. Mathematical approaches can be used to define how much effort is necessary to manipulate any given server. As such every single server *can* be manipulated with sufficient computing power.

Distributed ledgers[8] address these problems by raising the barriers for manipulation of stored data. In distributed ledgers many data storage points (nodes) are all connected with each other and store all data simultaneously, and together constitute the common ledger. DLT requires consensus of those nodes rather than just the confirmation by one hierarchically structured storage device, as with a centralised ledger. The technical details of how to achieve consensus vary – technology allows for instance for proof-of-work concepts[9], or proof-of-stake concepts.

Figure 1:



Adapted from Paul Baran, On Distributed Communication Networks, 1962

[8] For technical references in this part *see* Zetzsche, Buckley, Arner, *supra* note 7.

[9] In a proof-of-work system, multiple servers ('nodes') all try to solve one mathematical problem. The first node to solve the problem is compensated, while all others use the solution provided by the first node to verify that the problem has been correctly solved; thereby the solution to the mathematical problem assumes the function of a unique, one-time-use code.

Assume there are N nodes (rather than one centralised ledger) and E describes the effort necessary to break into any single server. Given that all other conditions (security of each server etc.) are equal, we would expect the efforts necessary to manipulate all servers linked in the ledger to be N x E rather than 1 x E. The number of servers that will need to be manipulated to manipulate the outcome will depend on the number of servers necessary for consensus and the number of nodes involved. If N>1 the distributed ledger is more secure than the concentrated one.

'Blockchain' refers to how data are stored on the ledger. Rather than being stored individually, data are stored in a block bundled with other data. The block serves as the container of multiple data points, and all blocks are stored in a specific order (the 'chain'). Each block contains a timestamp and a link to the previous block. Rather than manipulating one point alone, the bundling of multiple datasets in one block requires a cyber attack to manipulate the whole block of data as well as – due to the time stamp and link – the blocks before and after the attacked block.

B. Permissioned vs Permissionless DLTs

DLT can take various forms. In particular, DLT systems can be permissioned or permissionless. Permissioned systems are essentially private networks with a pre-defined governance structure where data authorisation depends upon the agreement of multiple pre-defined servers.

In contrast, permissionless blockchains such as Bitcoin operate on public domain software and allow anyone who downloads and runs the software to participate. In some cases even the code is further developed in the public domain. The participants in those distributed ledgers may not know who else is running a server functioning as a node at any given time. There is an additional security element in the unknown inherent in this structure: if the number of overall nodes is known a cyberattack may be planned with greater certainty given that the maximum number of nodes is certain.[10]

III. DLT and the Risks of Distributed Liability

DLT addresses the **storage trust issue**. DLT ensures the validity of datasets by spreading data over many nodes which have to agree, via the previously determined consensus mechanism, to confirm data validity. DLT can ensure better than other technologies that data are not manipulated while stored. DLT can also ensure that the party making a transfer has title on the ledger to the asset being transferred, and is not able to transfer it twice to separate buyers.

The important point here is that while DLT may enhance data security, it is not bullet proof. DLT has certain characteristics which could result in undesirable data distribution, data loss or data manipulation. All of these lead to questions about responsibility and liability, issues considered in this section.

A. Liability Risks Associated with DLT

DLT commonly gives rise to at least three major types of potential liability risk: ledger transparency risks, cyber risks and operational risks.

1. Risks from Increased Ledger Transparency

DLT stores data by spreading them over multiple nodes. Every node operator has access to the data stored on the ledger[11]. While data can be encrypted before being stored on a blockchain, rendering it effectively unreadable to third persons, meta-data is necessarily public. The enhanced level of transparency could enable re-personalisation of data stored on the distributed ledger, or enable nodes to make an informed guess as to identities entering into certain transactions.

[10] IT experts refer to this strategy as "security through obscurity".

[11] For instance, in Bitcoin, all the data is on the blockchain except the identity of the owners. To know that, one requires the private key. The private key is stored on the owner's wallet rather than the ledger. "However, anyone can see who owns each block, via its public header information, and can follow the links through the entire chain right back to the first block." *Cf*. Jude Umeh, *Blockchain Double Bubble or Double Trouble?*, 58:1 ITNOW 58 (2016).

Violation of Data Privacy

The transparency characteristics of distributed ledgers and data privacy are in tension. For instance, Bitcoin reveals considerable information about users' profiles, enabling repersonalisation of pseudonymous data. Indeed spreading data over multiple nodes may facilitate access to private data sets. Distribution of private data over the ledger could violate data protection laws. In some jurisdictions, penalties for violation of data protection rules are severe[12].

Another interference with privacy rights stems from the fact that data once stored on the ledger cannot be erased. The immutability feature of DLT is at odds with the 'right to be forgotten' granted in some jurisdictions, so victims will turn to damages instead. More significantly, this is directly at odds with the requirements of law that in some circumstances transactions are void, and title must be rectified to reflect this, for instance in the context of fraudulent transfers. Immutabilty and the requirements of law will clash.

Insider Trading and Market Abuse

If DLT is used to store sensitive, valuable information it may facilitate a range of financial abuses including insider trading, tipping and market manipulation[13]. Responsible entities may face severe civil and criminal penalties[14], and civil litigation in certain cases.

Identity Theft

While transparency is beneficial to data integrity it also facilitates access to assets through identity theft. In particular, if only the private key is required to divert assets and no central ledger authority is able to block access upon notice of loss, the private key itself becomes the target of illicit activities.

2. Cyber risks

Tampering with Data prior to Storage

DLT does not solve the general issue of data processing: inaccurate data remains inaccurate how ever it is stored. For instance, if data from a financial transaction are stored on a distributed ledger, the data will often be generated by just two entities, buyer and seller. If a so called Man-in-the-middle cyber attack focuses on the transacting parties, rather than the storage device (DLT), users relying on the ledger may not realise the inaccuracies and rely upon it. Permissionless distributed ledgers are particularly exposed due to non-existing user/client enrolment/ identity processes. That explains the attacks observed on the Bitcoin owner's wallet.

Brute Force Attack and Cheats

Even in what DLT is best at – safe storage – a distributed ledger has its limits. If all attacked nodes are of the same level of security as a centralised ledger, a brute force attack will require very significant effort from the attacker if all nodes are equally important and safe. Yet both conditions are unlikely to be true.

First, transaction logic will lead to concentration among the nodes making some more important than others. For instance, in some virtual currency blockchains, nodes are compensated per transaction they complete, thus providing incentives to compete for transactions. Some of the most active nodes will process a high proportion of transactions leading to a concentration of data generation on those nodes. For instance, in the blockchain that underlies Bitcoin just five mining pools together process approximately 85% of all mathematical problems, i.e. mining of coins. The ledger is partly recentralised. If consensus building is capacity oriented, as in some blockchains

[12] For instance, under the European Data Protection Regulation, regulators may impose penalties of up to 4 percent of a firm's turnover.

[13] *See* ESMA, *supra* note 2, at 11, ¶38.

[14] *See* 15 U.S. Code § 78u–1 (Civil penalties for insider trading), allowing the court to impose penalties three times the profit gained or loss avoided. Under European law the penalties amount to up to either 15% of the entity's turnover for insider dealing, unlawful disclosure and market manipulation, or €15 million, whatever is higher. See Market Abuse Regulation (EU) No 596/2014 Art 30(2).

including Bitcoin, the attack must only result in control over more computing power than is retained by honest nodes, an instance referred to as '51% attack'. Thus, a cyber attack that focuses on the handful or so of nodes in which most transactions are concentrated, is more likely to be successful. Or, since those brute force attacks require an enormous amount of computing power, an attacker could 'convince' the necessary number of nodes (or cheat those nodes) to adopt a different version of the ledger software through which the desired change is implemented.

Second, some nodes will be safer than others, given that some owners will invest more in cybersecurity than others. It is safe to assume that the majority of nodes managed by non-professional institutions will be less secure than the cyber fortresses typical of important centralised ledgers. Attacking the nodes with weaker security may be productive with less effort than that required for a brute force attack on all nodes simultaneously. These attacks promise better results when the attackers have access to any resource not available to others; one might think of advanced cryptoanalysis while the nodes' encryption has lower standards.

Double Spending and Distributed Denial of Service Attacks

Further potential liability events include double spending attacks where the same currency unit is simultaneously assigned to two different users so that both are under the impression of having received, and are able to spend, the same coin at the same time. One mechanism of self-defence foreseen by the Bitcoin core developers is that nefarious manipulation would lead to a general loss of trust, resulting in the plunge of the value of Bitcoin, thus presumably harming the attackers, who are also presumably heavily invested in Bitcoin. This disincentive is unlikely to stop attackers seeking to destroy the Bitcoin system as a form of terrorism, or to merely harm its users.

Another potential threat stems from distributed denial of service attacks (DDOS). Again, DDOS is the more dangerous the more concentrated the ledger. For instance, in the Bitcoin ledger where a handful of mining pools control by far the most computing power, DDOS could bring, and have frequently brought[15], mining to a halt.

The more DLT is widely spread in the business sector, the more likely it is that some rogue or terrorist may turn to DDOS. Even if immediately detected due to intense monitoring, the effects are potentially severe[16].

3. Operational Risks

Insufficient Coding

While the standardisation and automatisation that form part of DLT mitigate – in principle – operational risk, an error once implemented in the code may easily spread over the whole system affecting a greater number of nodes and individuals than a concentrated ledger. This creates serious problems in light of the fact that "there is no such thing as flawless software; there are always errors or 'bugs' that negatively affect the performance of the software or make it vulnerable to attack by hackers."[17]

[15] For instance, on March 7, 2015, five Bitcoin mining pools were subject to a DDOS attack that prevented miners from mining for six hours. The attacker demanded five to ten bitcoins to end the attack. *See* Julia McGovern, *Official Statement on the Last Week's DDoS-attack against GHash. IO Mining Pool*, CEX.IO (March 16, 2015), https://blog.cex.io/news/official-statement-on-the-last-weeks-ddos-attack-against-ghash-io-mining-pool-14156 (last visited June 30, 2017).

[16] For details *see* Zetzsche, Buckley, Arner, Zetzsche, Buckley, Arner, *supra* note 7.

[17] *See* Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 856 (2015). This is particularly true for the software underlying the Bitcoin system, *see* Walch, *supra* note 17, at 858 (detailing a list of bugs and identified fixes in n. 99-102). The statement counters the open source mantra according to which "the more eyes look at the code the more can fix and react".

In particular, poorly maintained, outdated or deficient code could open the door for system hacks, such as those that occurred in the Mt. Gox and DAO cases. Further, the governance deficiencies of permissionless ledgers may turn into real world issues in the context of insufficient coding. For instance, the hard fork that occured in the Bitcoin system on August 1st 2017 was due to a lack of consensus as to whether a specific update improved the system, or led to unqualified benefits for some users[18].

Key Person Risk

Distributed ledgers rely on sophisticated software codes that are permanently rewritten in an effort to improve performance and security. As with all software, few experts understand the structure, and even fewer are able to adapt it if weaknesses of the code become known. This is particularly true in the case of permissionless ledgers, such as Bitcoin. Even if the risk is mitigated in the Bitcoin ledger since all of the code is being made public, the core concern holds true: In all business organisations key people pose a risk to the organisation – they could become sick, tired, mentally unwell, subject to extortion or corruption. Regardless of the reason, if the trust put in key people is ill-placed, the ledger's security and reliability are at risk. If this happens questions will be asked as to who is accountable for the key person's underperformance or misconduct.

Negligent Performance

For large scale financial services data, security and processing speed are of the essence. Assuming that a distributed ledger ensures certain security and processing standards to market participants in an effort to enhance market share, the question of who is responsible will be asked if the ledger fails to meet these standards.

B. Legal Consequences

Even in light of its limits, DLT is likely the safest way to ensure that data are not modified. At the same time, DLT's limits lead to legal questions. In particular, if a system may be broken or inaccurate or private data are stored via a distributed ledger, the legal question of who will be liable for losses will arise.

This question is not easy to answer given that DLT is a technological, not a legal, concept. Operating a blockchain tells us, in the first instance, nothing about the legal scheme underpinning the blockchain. This has several implications.

1. Applicable Law

First, very few governments have as yet adopted a **Blockchain law**[19]. That does not mean, however, that no law applies or, as has been stated, law's focus needs to shift from individuals to (web) communities[20] – we pesky lawyers cannot be so easily sidelined. Rather, lawyers facing innovation look at the legal system as a whole and apply the system's foundational principles[21], and the law will provide an abundance of generally applicable principles, including the law of contracts, torts, property, partnerships and companies, some of which are enshrined in legislation while others (in particular in common law countries) are in case law which applies in the absence of specific legislation. Applying law to DLT will not be about novel legal institutions, but will entail applying general principles in the absence of specific legislation[22].

[18] *See* Tom Simonite, *Bitcoin is Spliting in Two. Now what?*, WIRED (Aug. 1, 2017), https://www.wired.com/story/bitcoin-is-splitting-in-two-now-what/ (last accessed Aug. 6, 2017).

[19] Arizona has adopted a blockchain law. Others are considering.

[20] *Cf.* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (arguing in favour of adaptation of the law to cyberspace).

[21] *Cf.* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996) (demonstrating the importance of principles); RICHARD A. EPSTEIN, SIMPLE RULES FOR A COMPLEX WORLD (1995) (stating that principles are well equipped to govern complex technical concepts).

[22] For instance, US courts and criminal enforcement agencies rigorously enforced criminal laws against Silk Road's master mind Ross William Ulbricht, fitting Bitcoin into existing jurisprudence. *See United States v. Ulbricht*, 31 F. Supp. 3d 540, 569 (S.D.N.Y. 2014); *United States v. Faiella*, 39 F. Supp. 3d 544 (S.D.N.Y. 2014); Edward D. Baker, *Trustless Property Systems and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange*, 45 SW. L. REV. 351, 372-374 (2015-16); V. Gerard Comizio, *Virtual Currencies: Growing Regulatory Framework and Challenges in the Emerging FinTech Ecosystem*, 21 N.C. BANKING INST. 131, 135-138, 141-146, 162 *et seq.* (2017); Raskin, *supra* note 6, at 980-983; Misha Tsukerman, *The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, 30 BERKELEY TECH. L. J. 1127, 1146-1159, 1166-1167 (2015).

2. Ledger Hierarchy

Second, DLT tells us nothing about the **entities involved** nor their **governance roles**. For instance, multiple servers functioning as nodes can belong to one legal entity (firm or person) or financial group or multiple unrelated owners. With regard to governance, in the case of permissionless blockchains, node owners typically will not even know who else is part of the blockchain, while a permissioned blockchain may have highly developed and legally sophisticated governance structures.

For the purpose of generalisation we rely on a **DLT hierarchy involving five groups**:

(1) the **core group** that sets up the code design and (de facto) governs the distributed ledger, for instance by having the technical ability and opinion leadership to prompt a 'hard fork' of the system (under certain conditions);

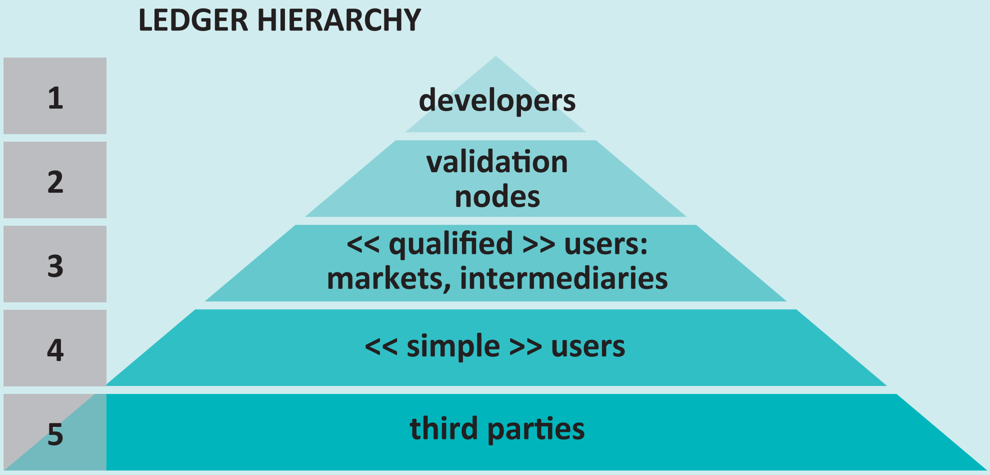
(2) the owners of additional servers running the distributed ledger code for **validation purposes** (such as Bitcoin nodes = owners, Ripple validation nodes etc.);

(3) 'qualified users' of the distributed ledger, such as exchanges, lending institutions, miners etc; and

(4) 'simple users' of the system, such as owners of Bitcoin[23], Ether or investors in the DAO;

(5) third parties affected by the system without directly relying on the technology, for instance counterparties of, and banks lending to, 'simple users', clients of intermediaries that clear their financial assets via DLT, clients of brokers that hold virtual currency on behalf of clients, etc.

Figure 2: Ledger Hierarchy



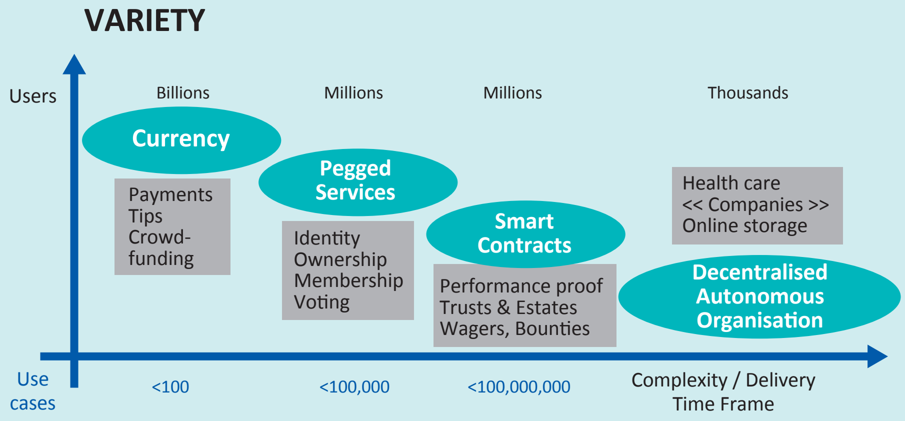
[23] In the Bitcoin ledger, validation nodes (element 2) and owners (element 3) are identical.

3. Variety

Third, DLT is a concept with **multiple variations**. From a distance Bitcoin, Ethereum, R3 and Ripple are all built on DLT so one is tempted to generalise, but up close they are very different animals. Generalisations are not warranted. Each DLT serves a certain use case which ranges from currency, pegged services, automatic execution of functions to permanent organisations.

Depending on the DLT's design and use case the number of users, the technical complexity and the delivery timeframe will vary – and so will the legal questions.

Figure 3: Blockchain Applications: End-User View[24]



Adapted from William Mougayar, *Understanding the Blockchain*, O'REILLY

C. Joint Control as Legal Qualification of a Blockchain

1. Application of Law to the Distributed Ledger

With regard to the question of the legal treatment of the cooperation underlying a distributed ledger, the type of cooperation created by code is of legal relevance[25]:

First, in general, law covers all relations among people and items owned and controlled by them. There is no carve-out for cooperation in a distributed ledger.

Second, no legislature is likely to enact an exception to this catch-all characteristic of law as it would promote irresponsible behaviour by those controlling the distributed ledger. No legal system could afford a carve out for DLT interactions.

Third, the discussion as to whether human beings are responsible for machines is long-standing, since at least the industrial revolution. In all jurisdictions of which we are aware the answer to this question has been the same: the law will cover, and be applied to, new situations and inventions appropriately modified to the new circumstances.

Fourth, individual transactions executed via a distributed ledger are likely to be contracts – with all related consequences, whether recorded only in code or in words. Each transaction is likely to give rise to liability in the event of failure; which will sound in real-world obligations, and potentially in bankruptcy.

[24] Taken from William Mougayar, *Understanding the Blockchain*, O'REILLY (Jan. 16, 2016), https://www.oreilly.com/ideas/understanding-the-blockchain (last visited June 30, 2017).

[25] For a discussion to what extend 'code is law' and how code drafting impacts BC law, *see* Zetzsche, Buckley, Arner, *supra* note 7; LAW SOCIETY, *supra* note 1, at 18-19.

The fact that law will apply is to be distinguished from the question of *which* law will apply. This will be determined by the application of the conflicts of law rules of the courts with potential jurisdiction over the matter, including their treatment of any choice of law provision in any agreement establishing the DLT[26].

2. Distributed Ledgers vs. Business Networks

From the outset, one is inclined to liken distributed ledgers to traditional 'business networks' (such as franchise systems, credit card networks and supply chains involving multiple parties). However, distributed ledgers differ from such traditional hybrid organisations[27] in one important respect: While all members of the network (e.g. franchisor and franchisees) are linked together by the common business interest (for instance, in the brand appeal), from a legal perspective traditional business networks follow the hub-and-spokes model, where the spokes (e.g. the franchisees) are connected to the other spokes only indirectly through a contractual relationship to the 'hub' (for instance, the franchisor)[28].

Rather than indirectly through a hub, in a distributed ledger all nodes (group 2 of our hierarchy) are linked together, in that they together communicate in the consensus process and thereby determine which data stored via the 'the common ledger' is right and wrong[29]. This connection removes the hierarchical relation derived from the hub to spoke characteristic for business networks and justifies the term 'peer-to-peer networks'. In turn we find no difference between horizontal and vertical anymore – all links to other nodes are by definition 'on the same level', pursuing a common objective. From a legal perspective, the connection provides the (in business networks: missing) link between the network partners. Where traditional business networks are mere virtual networks, distributed ledgers are 'real' networks – with a real physical (tech) link.

While distributed ledgers vary in terms of software processes and thus their legal qualification is likely to vary, we posit that legal consequences follow from this direct link among the nodes: It is the tipping point at which a loose assembly of self-interested entities turns into a group of entities legally tied together.

3. 'Shared control' as a Common Feature of Distributed Ledgers

The very fact of distribution among many ledgers which together perform a commercially relevant function renders legal consequence likely. At the same time, the joint performance assigns to all nodes together significant influence over all users' positions in that they can together exclude any single user from participation. For instance, if all but one user upload a new software version incompatible with the old one, the value of the remaining user's position in the ledger suffers. In most systems, agreement among a 51% majority of nodes or computing power is determinative. The operations of the information technologies interacting in a distributed ledger could be treated like those of the human beings controlling the servers and computers on which the software runs, or be treated like items a person is responsible for, similar to an animal or a car. In this case, the law would ask whether the person engaged in negligent conduct, i.e. violated a standard of care when the item inflicted harm on someone.

We infer from such quasi-organisational characteristics of the distributed ledger which go beyond mere economic interest that the whole ledger has a purpose or aim – the joint performance of the ledger service – from which obligations to cooperate and of loyalty as well as internal and external liability could follow.

Once it is established that distributed ledgers have a sufficiently close organisational relation (regardless of how this is legally interpreted in any

[26] LORD COLLINS, ET. AL., DICEY, MORRIS AND COLLINS ON THE CONFLICT OF LAWS (2016); ADRIAN BRIGGS, PRIVATE INTERNATIONAL LAW IN ENGLISH COURTS (2014); on choice of law in the blockchain context *see* LAW SOCIETY, *supra* note 1, at 10-13.

[27] Hugh Collins, *Introduction to Networks as Connected Contracts*, 11 *et seq.*, *in* GÜNTHER TEUBNER, NETWORKS AS CONNECTED CONTRACTS (2011).

[28] For details *see* Zetzsche, Buckley, Arner, *supra* note 7.

[29] Note that while depending on the server protocol and storage algorithm there may be difficulties to prove that any node X was *directly* in contact with any node Y, any node X runs code with which node Y was, or necessarily comes, into contact.

given jurisdiction) duties based on good faith as determined by the common good, liability among the ledgers (i.e. internal network liability) and liability to third parties (i.e. external network liability) could be presumed to arise. In turn, one node owes to the other loyalty (for instance, not to turn off the computer to maintain the network's processing efficiency or regular software and hardware updates to maintain the ledger's performance) and is directly liable for economic loss in case of its breach. Further, if a third party is damaged by inaccurate or insecure data storage which is, as was shown, possible, the third party could direct its claim based on **tort law or special liability statutes** to all nodes together.

This preliminary result arises in light of the six features of distributed ledgers including:

(1) joint access to data ('distributed');

(2) joint information about the process ('publicity'/'transparency');

(3) joint administration (in that no single ledger alone can determine the outcome) ('decentralised');

(4) joint development, i.e. to change the underlying code some consensus mechanism is necessary and no single node alone can determine the outcome;

(5) permanence – data cannot be erased, a permanent log is maintained in which all transactions may be tracked by order of processing; and

(6) verifiability – the above features combine to mean data cannot be amended while stored except through a major, trackable process ('immutability').

From a legal perspective some type of liability – joint, several or proportionate – could arise from this joint control towards third parties and among the nodes themselves. Which type of liability will arise will depend on the details of the DLT system, in particular the consensus mechanism, and on the rules of the specific applicable legal system or systems. However, our baseline position is that there are significant potential liability risks for entities involved in a distributed ledger, particularly those with design, control and/or maintenance roles.

D. Liability Risks in Major Legal Systems

Given that private law differs from country to country we will address the three main legal families in the world including **French civil law** based on the Code Civil (which extends to many Western European, African and South American countries), **Common Law** (as examples we address the US, the UK and Australia), and **Germanic civil law** which is influential in, besides Germany, Austria, the Netherlands, Switzerland, China, Japan and Turkey.

Of course, the specifics of each head of liability will be entirely jurisdiction specific, so our analysis is general, and intended to do no more than make the point that participants in a distributed ledger are highly likely to be potentially subject to liability, in one way or another, for their conduct. Proponents of DLT often like to pretend that the technology is somehow beyond the law, or at least, the law's reach. But courts will never allow such a restriction in their jurisdiction. The courts of sophisticated legal systems are jealous of the extent of their jurisdictions and for the very good reason that citizens should not be without redress in their nation's courts[30].

[30] *See The Eleftheria* [1970], at 94 (per Brandon J); *IRB-Brasil Resseguros, S.A. v Inepar Investments*, S.A. No. 191 (New York Court of Appeals).

1. Contract

In contract law each party is liable under the terms of the contract, i.e. for that which the contract says they are liable. The parties to the contract are not the computer as non-human electronic agent, but the person that exercises control (by virtue of ownership, management rights, or otherwise) of the non-human agent; the contractual acts – meeting of minds, breach of contract, performance – are attributed to this socio-technical ensemble[31]. In order to establish liability, a contract and a breach of the contract are required.

Without doubt both contract and breach may be established (and have been established[32]) in the relationship between groups 2-4 of our distributed ledger hierarchy, on the one side, and group 5 - the third parties - on the other. For instance, if the Bitcoin broker breaches its promise to hold a certain amount of virtual currency on behalf of its client the broker will be subject to a contractual claim by its client[33].

Beyond this obvious case contractual relations extend further into the direct relationships among groups 1 to 4 of our DLT hierarchy, given that both contract and breach can be established.

A **contractual agreement** requires an offer and acceptance (to establish mutual assent), consideration (anything of value exchanged) and an intention to create legal relations[34]. As to offer, acceptance and mutual assent: In our DLT hierarchy we suggest that hierarchy groups 1 and 2 – the core group and validation nodes – are parties to the 'distributed ledger contract' given that without them the system would not work[35]. Even if some members of DLT hierarchy groups 1 and 2 do not wish to enter into legally binding relations, the fact they participate in the system knowing that third parties will rely upon it, may turn their participation in the distributed ledger into legally consequential conduct[36]. In particular, in the Bitcoin blockchain individuals who wish to participate in the ledger join the network – and declare their consent to the disclosed *modus operandi* – by downloading the freely available Bitcoin software and thus volunteering their computer to run the Bitcoin ledger software.

Consideration matters in most common law systems. It may be less readily identifiable given the uncertain flows of assets in open source and permissionless systems, however, any type of consideration will suffice. Consideration can take the form of additional virtual assets (as in the case of Bitcoin miners), traffic on a website (for advertisement purposes) or fee payments. The fact participants willingly enter into a distributed ledger, suggests they perceive value from doing so. And of course in civilian legal systems, consideration is not usually a precondition for the existence of a contract.

[31] Günther Teubner, *Rights of Nun-Humans? Electronic Agents and Animals as new Actors in Politics and Law*, 33:4 J. L. & SOC'Y 497 (2006).

[32] *Cf.* the Bitcoin-denominated Ponzi scheme run by Trendon Shavers, who defrauded investors out of more than 700,000 Bitcoins. The respective SEC enforcement action resulted in an order to disgorge investments amounting to more than US$40 million and a civil penalty of US$150,000 to be paid by both Shavers and the investment vehicle set up by him, *see SEC v. Shavers*, No. 4:13-CV-416, 2014 WL 4652121 (E.D. Tex. Sept. 18, 2014); U.S. Securities and Exchange Commission, Litigation Release No. 23090 / Sept. 22 (2014), *Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust*, Civil Action No. 4:13-CV-416.

[33] *Cf.* Bayern, *supra* note 6, at 25-29; LAW SOCIETY, *supra* note 1, at 16-18 (discussing liability of token issuers and redemption requirements).

[34] *See* from the old English case law: *Household Fire and Carriage Accident Insurance Co Ltd v. Grant* 4 Ex D 216 (1879) (Thesiger LJ); *Carlill v. Carbolic Smoke Ball Company* 1 QB 256 (1893) (Bowen LJ); on the German civil code: *Busche in Münchener Kommentar zum Bürgerlichen Gesetzbuch*, 7th ed. 2015, Vor §145 ¶31; and on the French Code Civil: *Case Société Chronopost v. Société Banchereau*, N ° of appeals: 93-18632 (1996).

[35] Even if we do not consider the validation nodes parties to the DL 'contract', their conduct may matter if we include them as agents to the core group.

[36] The legal basis for that may vary. In the UK or Australia such conduct could give rise to remedies under statutory law, *see infra* at D.2. In the US, an implied contract is likely to be found to exist, *see* USC, in *re Baltimore & Ohio R. Co. v. United States*, 261 U.S. 592, 597, 58 Ct.Cl. 709, 43 S.Ct. 425, 67 L.Ed. 816 (1923) (holding that "an agreement … is inferred, as a fact, from conduct of the parties showing, in the light of the surrounding circumstances, their tacit understanding").

Second, whether there is a **breach of contract** depends on conduct in the context of the contract's terms. General principles of contract law apply: Whether a term is a condition or a warranty depends on the intentions of the party discerned from the contract in light of context. The more important such features are for one party, and the more clearly they are expressed prior to entering into the agreement, the greater the likelihood that judges will consider them as part of the contract. Warning language displayed prior to entering into the contract may constitute terms. Disclaimers and liability waivers may further limit obligations *if* they are upheld in court[37]. For contractual liability, however, it makes no difference whether the damage resulted from the misconduct of a human being or a machine's malfunction. The owner or operator is liable for the machine's malfunction.

Contractual liability results in **joint liability** where the causes of actions are not distinct and the defendants acted in furtherance of a common purpose. Generally speaking all multiple nodes functioning together to run the ledger (hierarchy group 2), and all core developers developing the code together (hierarchy group 1) would meet that test on their respective hierarchy level. If nodes and developers cooperate, hierarchy groups 1 and 2 may find themselves tied together by joint liability vis-a-vis third parties.

Some authors suggest **no contractual relationship exists** in distributed networks where the user is unknown and the userbase unstable, where the performance of the service depends on who is connected at what time, and none of the individual nodes is in itself essential (such as in permissionless blockchains like Bitcoin)[38]. Proponents of the idea that the DLT relationship does not give rise to legal rights refer implicitly to participants' lack of intent to grant contractual rights to co-users[39]. However, business entities are often unaware of all participants, and their roles, in complex business interactions. A distributed ledger is a complex network of users and contractual relationships that may change from time to time depending on who is participating in the ledger operation. While anonymity of the parties renders enforcement potentially difficult, it does not mean the actions of individuals who together 'operate' the distributed ledger are not legally revelant.

[37] General Public License or Open Source Software Licenses (OSSL) used by open source developers, including those that distributed the codes of Bitcoin and ETHER, use very broad language to limit liability. It is uncertain, however, whether courts will listen to this argument. In particular, legislation in some countries provides for certain non-excludable warranties where a firm is carrying on a business. For instance, the U.S. Uniform Commercial Code § 2-314 to § 2-316 provides that certain warranties are implied in the sale of a product (as adopted by U.S. states); the Australian *Competition And Consumer Act 2010* (Cth) sch 2 s 54 stipulates that there "is a guarantee that the goods are of acceptable quality." In light of such statutes, the exclusion clauses may not be effective in limiting liability for negligence and consequential damages.

[38] Mélanie Dulong de Rosnay, *Peer-to-Peer as a Design Principle for Law*: *Distribute the Law*, 6 J. PEER PROD. 2 sub. 2 (2015), *available at* http://peerproduction.net/issues/issue-6-disruption-and-the-law/peer-reviewed-articles/peer-to-peer-as-a-design-principle-for-law-distribute-the-law/; Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia,* 55 (Unpublished manuscript, March 12, 2015), *available at* https://ssrn.com/abstract=2580664; Bayern, *supra* note 6, at 31-33.

[39] Bayern, *supra* note 6, at 31-33 (arguing that "a bitcoin does not represent a transactional or organizational right in the way that shares of stock or a partnership interests do" and stating that "given merely my knowledge of a secret key for a certain amount of bitcoins, there is nobody associated with Bitcoin against whom I have a claim-right, and conversely nobody has a duty to me – apart from the general duty to refrain from interfering with intangible personal property. Those running the Bitcoin software are free to ignore my attempts to transfer bitcoins to a new bitcoin address. They have no contract with me, implied or otherwise. They are free to ignore me, to dispute my ownership of bitcoins on technological grounds, and so on. … In this sense, a bitcoin is not a right against the other users of the Bitcoin network").

In a distributed ledger, electronic messages and transactions coincide; any message a node sends is a declaration of intent and contribution to the transaction[40]. It is inconsistent to deny legal relevance of cooperation where only reliance on others ensures access to, and transfer of[41], one's own asset value and where this very cooperation by others is the precondition of contributing to the ledger in the first place. A simple example may demonstrate our point: assume miners on the Bitcoin blockchain find, for whatever reason, that no one will accept (today) the newly and properly generated Bitcoins, or (after 21 million Bitcoins are mined) who will accept the recycled Bitcoins, effectively creating a fork between the blockchain leading to this miner and all others. The miner who invested significant processing power (i.e. energy) will either turn to the Bitcoin nodes that validate honestly mined coins (i.e. all who hold Bitcoins directly) for fulfilment of the promise given to them that honestly mined coins would become part of the chain and accepted by others as currency, receive value, or to the core developers, for damages. In both cases the miner has standing to sue based on the promise received by all Bitcoin nodes together, regardless of the fact that the miner did not, at the time, know the nodes nor the developers. While enforcement may be difficult, we must not confuse potential for legal liability with the challenge of *enforcement*.

Another argument against contractual liability is that node operators may have no way of knowing to which use their fragmented contribution to the network is put, which for instance could include money laundering or terrorist financing. Again, this argument is flawed. Nodes *could* require AML/CFT checks as a precondition for hard currency being exchanged into virtual assets – they could define this as a precondition for the overall use of the networks. The fact that nodes sign up to the network, in particular when they buy/sell/mine Bitcoins without AML/CFT checks may evidence ignorance of the law but not the law's inapplicability.

2. Law of Torts/Delict and Special Liability Statutes

Joint tortfeasors are two or more individuals with joint and several liability in tort for the same injury to the same person or property. Joint and several liability means the plaintiffs can collect any damages award from any one of a group of joint tortfeasors. Tort claims are particularly important where there is no contractual liability, in particular with regard to DLT hierarchy group 5 suing the other DLT hierarchies, or in the case of DLT hierarchy groups 1 and 2 being sued by DLT hierarchy groups 3 and 4 in the absence of a contract[42].

[40] This concept is inherent in automatized transactions. *See*, on smart contracts: Koulu, *Blockchains and Online Dispute Resolutions: Smart Contracts as an Alternative to Enforcement*, 13 SCRIPTED 40, 61 (2016) ("A transaction is a message, a message is a transaction. … By making the transaction, each party enters into a contract") and at 65 ("the declaration of intent is given through a transaction to the contract itself"); LAW SOCIETY, *supra* note 1, at 21-22.

[41] Note that the person who sends the message to be incorporated into the blockchain is not the person who wants to receive a bitcoin, but the person who wants to relinquish it. *See* e.g. Sveriges Riksbank, *Financial Infrastructure Report* (2016), http://www.riksbank.se/Documents/Rapporter/Fin_infra/2016/rap_finansiell_infrastruktur_160426_eng.pdf ("A transaction starts with a party that wishes to execute a payment, for instance, proposing the transaction to the network by sending a transaction instruction to the computers included in the network. Each participant in the network has a unique pair of keys that are used for encryption and it is through these that the participant can be identified in a secure manner … The network checks that the transaction information is correct, for example that the recipient exists and that the sender owns the asset to which the transaction refers.").

[42] *See* Primavera De Filippi, *Ethereum*, 100, *in* ABÉCÉDAIRE DES ARCHITECTURES DISTRIBUÉES (Cécile Méadel & Francesca Musiani eds., 2015) (arguing in favor of tort claims against DAO developers); Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 55-56 (Unpublished manuscript, March 12, 2015), *available at* https://ssrn.com/abstract=2580664 (arguing in favor of the developer's liability and against the user's liability since the user did not know, or did not have a good reason to believe that the third party could potentially cause harm to someone); Francesca Musiani, Cécile Méadel, Alexandre Mallard, *Bitcoin*, 45-46, *in* ABÉCÉDAIRE DES ARCHITECTURES DISTRIBUÉES (Cécile Méadel & Francesca Musiani eds., 2015) (considering tort claims against Bitcoin code developers, while denying them against miners, nodes and owners of BTC); LAW SOCIETY, *supra* note 1, at 7-11, 19 (discussing tort liability in the Blockchain).

While the importance of these claims varies across jurisdictions – in many common and German-law based civil law jurisdictions the courts are loathe to award damages in tort for pure economic loss – the type of loss to which most risks will give rise. On the one hand tort claims could arise from damages to 'property' via the distributed ledger. The relevance of property-related claims depends on the legal qualification of the plaintiff's position in the system. For instance, if a Bitcoin is deemed tangible property[43] intentional interference (i.e. a hack or hard fork resulting in temporary denial of access or even permanent diversion of the Bitcoin owned by the user) could result in claims based on trespass to chattels or conversion[44], while the application of tort law to Bitcoin as intangible property[45] is less certain[46]. On the other hand, claims could stem from fraud, theft or other types of illicit conduct. Code modification could amount to any of the former. Whether code modification in fact amounts to fraud or other types of actionable harm depends, among other things, on the users' intention. In most jurisdictions, intentionally inflicting harm on others results in liability for damages[47].

An entity operating in the distributed ledger may be liable in tort if its negligent act, omission or misstatement causes loss or damage, including loss due to a security breach or a coding error. A record on the system may be inaccurate causing losses to those relying on it[48]. An entity's liability in negligence will depend on whether it owes a duty of care and has breached that duty, whether the breach caused loss or damage, and whether it has effectively contractually excluded liability for this type of loss or damage.

The existence of a duty of care depends in part on the type of loss suffered and by whom it is suffered. In most potential distributed ledger actions, the relevant loss is likely to be 'pure economic loss' (that is, economic loss occurring in the absence of, or prior to, any damage to property or person). Courts in common law countries (and many civil law countries) have been reluctant to find that a duty of care exists in cases of pure economic loss for fear of "imposing unreasonable burdens on the freedom of individuals to protect or pursue their own legitimate social and business interests ..."[49]. However, one may be liable in negligence for pure economic loss in certain situations, especially if the plaintiff was a member of a class exposed to foreseeable loss by the defendant's conduct whose members were ascertainable by the defendant and if imposing

[43] *Cf.* Raskin, *supra* note 6, at 984-1005 (arguing that Bitcoin is tangible property for the purposes of Civil Procedure due to the exclusionary effect of the "owner's" access key and in favor of allocating jurisdiction based on rights *in rem*). Raskin's opinion is shared by the US Internal Revenue Service, *see* US Internal Revenue Service, *Notice 2014-21 IRS Virtual Currency Guidance* (March 25, 2014) https://www.irs.gov/irb/2014-16_IRB/ar12.html (arguing that virtual currency is property for tax purposes). But, *see* Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, 24:1 U. MIAMI BUS. L. REV. 1, 14-27 (2016) (arguing that Bitcoin is not "money" under the US Uniform Commercial Code since the Bitcoin owner lacks physical custody). *See also* Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*, 17 NEV. L. J. 139, 179-180 (2016) (undecided).

[44] *See* on the US: The Restatement (Second) of Torts § 217 and § 218; on Australia: *Penfolds Wines Pty Ltd v Elliott* (1946) 74 CLR 204; and on the UK: *Torts (Interference With Goods) Act 1977* (UK).

[45] *Cf.* Bayern, *supra* note 6, at 29-31 (holding that a Bitcoin is intangible personal property); Schroeder, *supra* note 43, at 23-42 (arguing that Bitcoin is a "general intangible" under the US Uniform Commercial Code).

[46] The answer partly depends on whether property doctrine such as trespass to chattel may be expanded into the electronic context. The case law and articles are too numerous to be discussed here in detail. For an overview from the US perspective, *see* David M. Fritch, *Click Here For Lawsuit – Trespass to Chattels in Cyberspace*, 9 J. TECH. L. & POL'Y 31 (2004); Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L. J. 421 (2002).

[47] See for the common law: Bayern, *supra* note 6, at 33 note 28 (holding that "interference with individually owned bitcoins via a technological vulnerability on the owner's computer system probably amounts to conversion"). On German civil law, *see* s. 826 of the Bürgerliches Gesetzbuch, § 1295 (2) of the Austrian Allgemeines Bürgerliches Gesetzbuch (General Civil Law Book) (granting damages for pure economic loss). See articles 1382 and 1383 of the French Code civil. See Edward A. Tomlinson, *Tort Liability in France for the Act of Things: A Study of Judicial Lawmaking*, 48 L.A. L. REV. 1299-1367, 1314 (1988).

[48] *See* Vernon Valentine Palmer, *A Comparative Law Sketch of Pure Economic Loss*, 305-6, *in* COMPARATIVE TORT LAW: GLOBAL PERSPECTIVES (Mauro Bussani & Anthony J. Sebok, eds., 2015), regarding potential liability for flawed data on which other parties rely.

[49] *Perre v Apand* (1999) 198 CLR 180, 218. *See id*., at 315 *et seq*.

the duty does not unreasonably interfere with the defendant's commercial freedom[50]. Some common law countries also have statutory provisions that extend the duty of care to apply in cases of pure economic loss. For example, in New South Wales in Australia, the Civil Liability Act of 2002 includes 'economic loss' in the definition of 'harm' and a person may be negligent in failing to take precautions against a risk of harm if the risk was foreseeable and not insignificant, and a reasonable person in the person's position would have taken those precautions[51].

The relevant operator might establish that no duty of care existed, particularly if the plaintiff is a second or third line victim and not part of an ascertainable class. Liability for pure economic loss is therefore more likely in the case of smaller, permission-based blockchains where the class of plaintiffs is readily ascertainable, although the plaintiff would still need to prove the entity breached its duty of care (by, for instance, not meeting the standard of a reasonable node or software developer) and that this breach caused the plaintiff's loss[52]. Operators may contractually exclude liability for negligence in these situations. However, such an exclusion clause may be void under consumer legislation or subject to narrow construction by the courts.

Over time, and painfully slowly from the perspective of technical innovation, courts in jurisdictions that allow tort claims for pure economic loss will shape the duties of care in the DLT context as distributed ledgers gain importance in business over time. This could result, for instance, in judicial pronouncements regarding the appropriate announcement time and method for code modifications, the required bit size and node computing power for the modification, and the necessary diligence prior to the new code's release. In a way, the strictest jurisdiction involved may determine the level of care for the whole ledger as law suits will be filed there.

The important point here is, again, that groups 1 to 4 in our DLT hierarchy cannot act as they wish; rather they need to keep the reasonable expectations of all parties relying on the respective ledger as well as the evolving case law in all jurisdictions where system users and beneficiaries can establish a court's jurisdiction in mind, and risk liability if they do not.

3. General Partnership or Joint venture

The criteria of partnership law as to when a group of joint actors will be a partnership differ from jurisdiction to jurisdiction. While under the laws of some jurisdictions[53] the **joint pursuit of a (joint) objective** suffices to establish an unincorporated company[54], the law of most common law jurisdictions require for a general partnership the **sharing of profits**. If a cooperation is a partnership it will usually result in joint liability.

[50] *Perre v Apand* (1999) 198 CLR 180, 204.

[51] For example, *see* ss. 5, 5B(1) of the *Civil Liability Act 2002* (NSW).

[52] *See* John C. P. Goldberg & Benjamin C. Zipursky, *Torts as Wrongs*, TEXAS L. REV. 88 (2010).

[53] Notably, German law on the Gesellschaft bürgerlichen Rechts ("unincorporated company"). In particular, it has been held that certain developer associations in the open source domain such as the Apache Software Foundation or core developer groups qualify as unincorporated companies if in addition to the joint purpose of further developing an open source software there is some, albeit purely factual, organizational structure. *See* TILL JAEGER & AXEL METZGER, OPEN SOURCE SOFTWARE ¶193-200 (4th ed., 2016). The same applies to Blockchain core developer groups surrounding Bitcoin and Ethereum, in particular the Bitcoin foundation.

[54] *See*, for instance, s. 705 of the German Civil Code and article 1832 and 1833 of the French Civil Code. Absent specific stipulations the French law assumes that both profits and liability are to be distributed according to the size of the contribution of every partner. Further, under article 1833, a partnership's object has to be legitimate and in the partners' interest. In the case of a partnership (société de personnes) the *intuitu personæ* is determinative, meaning that the contract can be declared void in case of an error concerning the qualities or capacities of a putative partner, as ruled by the Cour de cassation (Com. 8 mars 1965, Bull. civ. III, n° 173, p. 147.

For instance, while participation in a clearing and settlement distributed ledger system that relies on all nodes' mutual cooperation for identifying true transactions may be deemed a joint pursuit of a shared objective sufficient under some civil laws to establish a joint venture[55], the fee and profit sharing agreement will determine whether such a blockchain is deemed a partnership under common law. As long as profit opportunities are held by a third-party distributed ledger sponsor/organiser and the nodes bear their own expenses and are rewarded on predetermined basis as with Bitcoin, the risk that the system is a partnership at common law is very low indeed[56]. However, if in a permissioned blockchain the network of validation nodes offers the services of the network to third party users which pay 'the network' for these services, the system may be deemed a partnership; and in turn all validation nodes as partners may be liable vis-à-vis third parties.

While the former shows that there is significant liability risk, the **case of the DAO** illustrates the potential magnitude of the risk. In the DAO, all investors jointly voted on investment proposals, all held jointly the assets acquired, no legal entity was positioned as a liability shield in between assets and investors, and all investors agreed that they were to share the profits generated by the assets. If the DAO's assets had generated losses rather than profits (for instance, people working in a factory held by the DAO were harmed by an accident) all investors could be held to be partners and personally liable[57].

As a rule of thumb the risk of liability associated with DLT participation based on partnership law is the greater:

- the more a server owner benefits from participating in the distributed ledger through profits (as long as there are others who benefit in the same way);
- the greater its influence on the server design, set-up or update, with 'creators' being more influential than 'simple users'; and
- the greater its influence on the decision to let others use or be excluded from using the distributed ledger.

From the last consideration follows that the function of a validation node in a permissioned blockchain with a veto right against access or updates (hereinafter called 'consortium blockchain') is more likely to lead to personal liability than the 'simple' mining function in Bitcoin. The result of the former may well be not only mutualisation of data processing but also mutualisation of liabilities and risks.

4. Specific Legislation, in particular Competition Law

Regulators have suggested that DLT can pose a risk to fair competition and orderly markets. For example:

ESMA anticipates … [e]arly [DLT] participants might refuse or impose conditions on new members that make it unduly difficult or costly for them to join the DLT network. … Also, it may become increasingly difficult to develop competing systems through time for cost or technical reasons, e.g., patents that would protect certain components of the technology or the need to ensure interoperability with existing systems. This could drive some firms out of the market and lead to a monopoly-like situation with negative consequences on the cost and quality of the services.[58]

[55] An example could be provided by the Swiss giro network case BGE 121 III 310, 314-15 where the Swiss Federal Court has taken the view that for purposes of external liability the network should not be regarded as a collection of bilateral contracts but as a multilateral co-operative system similar to an unincorporated business organization; the argument rests on the ground that one bank could not meet its obligation without the other so co-operation was an implicit condition of the contract. On the common law perspective, see Hugh Collins, *Introduction to Networks as Connected Contracts,* 11 *et seq., in* GÜNTHER TEUBNER, NETWORKS AS CONNECTED CONTRACTS 64-71 (2011) ("Such a radical departure from the ordinary principles of contractual responsibility seems unlikely to be imitated in the common law").

[56] Other features missing in permissionless systems may include the lack of a centralized coordinating authority that receives and distributes the residual profits.

[57] This view has been shared by Andrew Hinkes, *The Law of The DAO*, CoinDesk (May 19, 2016), http://www.coindesk.com/the-law-of-the-dao/ (last visited June 16, 2017).

[58] *See* ESMA, *supra* note 2, at 11, ¶37.

If DLT functions as a technological barrier that enables or facilitates monopolies, additional liability may stem from competition/antitrust law. This is of great importance since competition laws often impose antitrust liability on different criteria from contract or tort law. For instance, under European competition law the definition of the responsible party ("enterprise") may include the parent, sister and subsidiary companies as well as significant shareholders of the former if they participated in, or benefitted from, the anti-competitive conduct, or directed and steered the entity involved in it[59].

Market participants involved in a distributed ledger system must keep this and other conduct-related legislation (such as data protection, copyright laws, consumer protection laws, tax laws, AML/CFT, landlord-tenant laws[60] etc.) in mind.

IV. Impact on Blockchain Participants

Given that there is liability risk to entities involved in or in contact with a DLT system, participants as well as regulators are well advised to take legal as well as technical precautions.

A. Participation as Operational Risk Contingent Liability

Centralised ledgers not only centralise processes, but also liability. Formerly, when looking at central counterparties market participants did not only pay for processing, but also for the risk cushion provided by one highly regulated, super secure and very solvent entity. Blockchain has the potential to mutualise control over these entities. However, under legal principles all over the world, joint control is likely to come along with joint liability. In a non-technical sense, participation brings about a contingent liability which needs to be considered as part of the IT-based operational risk.

B. Provisioning against Risk: Capital Requirements and/or Insurance

The Basel 3 capital adequacy rules while recognising information systems and IT importance treat such risks as but one type of operational risk.[61] As a principle banks must hold capital against operational risk[62]. Given the expected large loss impact and frequency of events, and the intermediary's collection of all risk-related events in few global databases[63], recognition of DLT risk and a predetermined risk budget similar to that for participation in a syndicate or other types of joint ventures could well be the outcome. Related concerns arise particularly in the context of systems which could be classified as financial infrastructure. Financial infrastructure attracts separate and additional requirements under guidelines from IOSCO and the Committee on Payment and Market Infrastructures (CPMI) of the Bank for Internatioanl Settlements (BIS)[64]. The CPMI principles contain detailed requirements in terms of capital, risk management etc which would clearly apply in the context of DLT-based payment and securities settlement systems.

[59] See Articles 101, 102 and 106 of TFEU in the Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01; W. P. Wils, *The Undertaking as Subject of E.C. Competition Law and the Imputation of Infringements to Natural or Legal Persons*, EUR. L. REV 25, 99-116, 100 (2000); *see also* Pieter Van Cleynenbreugel, *Single Entity Tests in US Antitrust and EU Competition Law* (Working Paper, June 21, 2011), *available at* https://ssrn.com/abstract=1889232, on the EU-US differences. However, DLT may also contribute to competition law compliance efficacy, *see* Ajinkya Mahesh Tulpule, *Enforcement and Compliance in a Blockchain(ed) World*, 1 CPI ANTITRUST CHRONICLE 45 (2017).

[60] *Cf.* Christopher, *supra* note 43, at 155 (arguing that access to an apartment governed by a blockchain may violate landlord-tenant laws if the blockchain inhibits the tenant's access following the tenant's default).

[61] *See* Vlasta Svatá & Martin Fleischmann, *IS/IT Risk Management in Banking Industry*, 2011 ACTA OECONOMICA PRAGENSIA 3, 42-60 (2011) (stating that current treatment of IS/IT-based risk is inadequate). To this day, the Basel risk management website has not devoted a special workflow to IS/IT risk, *see Basel Committee – Risk Management*, BANK FOR INTERNATIONAL SETTLEMENTS, http://www.bis.org/list/bcbs/tid_50/index.htm (last visited July 23, 2017).

[62] *See* BASEL COMMITTEE ON BANKING SUPERVISION, STANDARDISED MEASUREMENT APPROACH FOR OPERATIONAL RISK (March 2016), *available at* http://www.bis.org/bcbs/publ/d355.pdf.

[63] Marco Folpmers, *Basel's New Approach to Operational Risk: A Step Backwards*, GARP (April 22, 2016), http://www.garp.org/#!/risk-intelligence/all/all/a1Z40000003CA7oEAG/basels-new-approach-operational-risk (last visited July 10, 2017) ("Since banks struggle with the collection of sufficient loss data, consortia (such as ORX) have arisen in which banks pool operational loss data").

[64] *Principles for Financial Market Infrastructures*, BANK FOR INTERNATIONAL SETTLEMENTS (Dec. 2015), http://www.bis.org/cpmi/info_pfmi.htm?m=3%7C16%7C598 (last visited July 23, 2017).

Even in the absence of capital adequacy rules, given that losses from DLT participation can be serious enough and sufficiently likely to be considered by top management, a financial intermediary's management could be required to establish a DLT-related risk budget, enter into insurance, or limit DLT participation to very large and established counterparties. Be this as it may, DL participation does not come for free and requires consideration of each function in the DLT hierarchy and whether it adds to, or reduces, liability risk.

C. Distributed Ledger – Concentrated Ownership?

Liability matters little for a private party (an individual) with few assets who is therefore unlikely to become the target of a law suit (with anarchic code developers being an eminent example). Legal uncertainty, ambiguity and lack of assets can function as a liability shield for individuals as the reward will not justify the costs of enforcement. The perspective of a globally operating financial or production conglomerate is different: those entities are likely targets of lawsuits, regardless of the little legal certainty provided by legislation and case law. This could lead to risk multiplication given that someone may test the waters, and thereby influence the set-up of any distributed ledger, and potentially limit the use cases of DLT. Given the international dimension the legal assessments necessary to provide a full view of liability risk include the laws of multiple jurisdictions. This is particularly true of a permissionless blockchain. All of this together turns the drafting of access terms, and decisions while part of the system, into complex and costly endeavours.

Both liability exposure and transaction costs for its assessment have implications for the ideal *legal* set-up of a DLT structure. As such, we may observe that the ideal setting could – ironically – take the form of a concentrated legal structure in a distributed ledger system.

Concentration may be achieved by two means. First, participation in the distributed ledger may be limited to controlled entities of a conglomerate. Second, multiple parties jointly interested in one service could leave the set-up and operation of the system to one global enterprise sufficiently large and capitalised to bear liability risk and acquire those services on a fee basis, or set up and capitalise such an entity as a joint venture themselves.[65]

V. Law as a Factor in DLT Structuring

Risk does not vanish simply due to the use of a blockchain. Our analysis of the laws of the most important legal systems has revealed four general principles as to liability.

First, the more the ledger is organised or based on a predetermined governance structure (most evident in permissioned ledgers), the greater the risk that participants, in particular those participants that are influential and 'control' the ledger, will be held liable for breach of contract or as partners of the 'ledger partnership'. Second, cooperation of sophisticated financial and business services requires organisation and, if the resource dealt with by the ledger is essential, investors will demand control rights in return for their investment. Common sense and economic need will push for permissioned ledgers, so liability will be a major factor. Large scale economic use of the ledger will come with potential liability. Third, permissionless ledgers are not the answer to the liability issue. Even in unpermissioned ledgers (for instance Bitcoin), the liability risk is not zero, but rather highly case specific. There is a strong differentiation of treatment among countries and low levels of legal certainty; and thus higher legal costs and risk premia, especially for transnational permissionless systems. Fourth, our thesis that liability matters in the establishment of distributed ledgers holds nothwithstanding that the legal basis for liability will vary across jurisdictions. Some liability will arise from contract or liability statutes, some from special legislation, and some from tort or partnership law, but the net result of the joint/coordinated activity will most often be joint liability.

[65] For details *see* Zetzsche, Buckley, Arner, *supra* note 7.

From the perspective of globally active financial institutions and multinational enterprises that liability can result in different ways legally makes it far more difficult to enter into distributed ledgers across countries and with other firms. The risk of entangling one's own balance sheet with other ledger parties' obligations is a serious barrier to cross-firm ledgers.

Firms will try to mitigate these risks with choice of law and jurisdiction clauses, but this approach will be less effective with statutory, tortious and partnership liability and with services offered to consumers (given the mandatory jurisdiction and applicable law typically associated with consumer transactions). Parties will choose the governing law to minimise liability, but liability risk may well harm, in particular, the development of cross-border ledger systems with many nodes.

The risk of distributed liability of distributed ledgers suggests that concentrated ownership is the most likely way of legally structuring distributed ledgers. Distributed ownership may be conditioned on a higher degree of legal certainty and a greater degree of harmonisation across countries. Harmonisation of private law consequences of DLT systems could be most useful, although of course this will be a long-term undertaking[66]. In addition, international regulatory cooperation in development of minimum regulatory standards will be key to addressing potential risks, and this begins with the technical harmonisation presently underway[67].

From a legal and regulatory perspective, the starting point must be to focus on the sorts of issues that will arise when any of the core attributes which make DLT systems attractive – namely their security, immutability and transparency – fail, as fail they will.

As a result, DLT will have different impacts than many expect. In particular, liability will not be eliminated, but may instead be spread across the system, and financial intermediaries involved in a distributed ledger should arguably hold capital or acquire insurance for contingent liabilities stemming from DLT participation. Likewise, operators may, in time, need to be governed by regulatory requirements similar to those governing other providers of potentially systemically important infrastructure, such as traditional centralised payment and settlement systems.

Part of the thrill of blockchain to date has been its disregard of the law. With law in the picture, data are less attractively housed in distributed ledgers. This does not mean liability will exist in all cases. However liability matters, and distributed ledgers may, in time, most often be legally structured (particularly in permissioned systems) as a joint venture where all servers are owned and operated – ironically – by one entity, or a small number of specified entities, rather than as a cooperation among multiple and for the most part anonymous entities.

The authors gratefully acknowledge the financial support of the following: the Luxembourg National Research Fund, project "A new lane for Fintechs – SMART Regulation", INTER/MOBILITY/16/11406511; the Australian Research Council, project "Regulating a Revolution: A New Regulatory Model for Digital Finance"; and the Hong Kong Research Grants Council Theme-based Research Scheme, project "Enhancing Hong Kong's Future as a Leading International Financial Centre"; and the research assistance of Katharine Kemp, Jessica Chapman, Tsany Ratna Dewi, Paul Friedrich and Cheng-Yun Tsang.

The authors are grateful for comments and remarks provided by Jànos Barberis, Iris Barsan, Isabelle Corbisiere, Scott Farrell, Holger Fleischer, Annabel Griffin, Rob Hanson, Katja Langenbucher, Alain Pietrancosta, Gerald Spindler, Erik P.M. Vermeulen, Markus Willms, as well as participants at conferences and workshops organised by IJRS Sorbonne-Paris I, the Max Planck Institute for Comparative and International Private Law, Humboldt University Berlin, Tilburg University, University of Luxembourg. All responsibility is the authors'.

[66] *See* Paech, *supra* note 6, at 32-37 (examining options available under private international law to allocate blockchain arrangements across jurisdictions).

[67] The International Organization for Standardization (ISO) has established a new technical committee to work on the harmonization of standards for blockchain and DLT, with Australia as the chair, *see ISO/TC 307: Blockchain and Distributed Ledger Technologies*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, https://www.iso.org/committee/6266604.html.