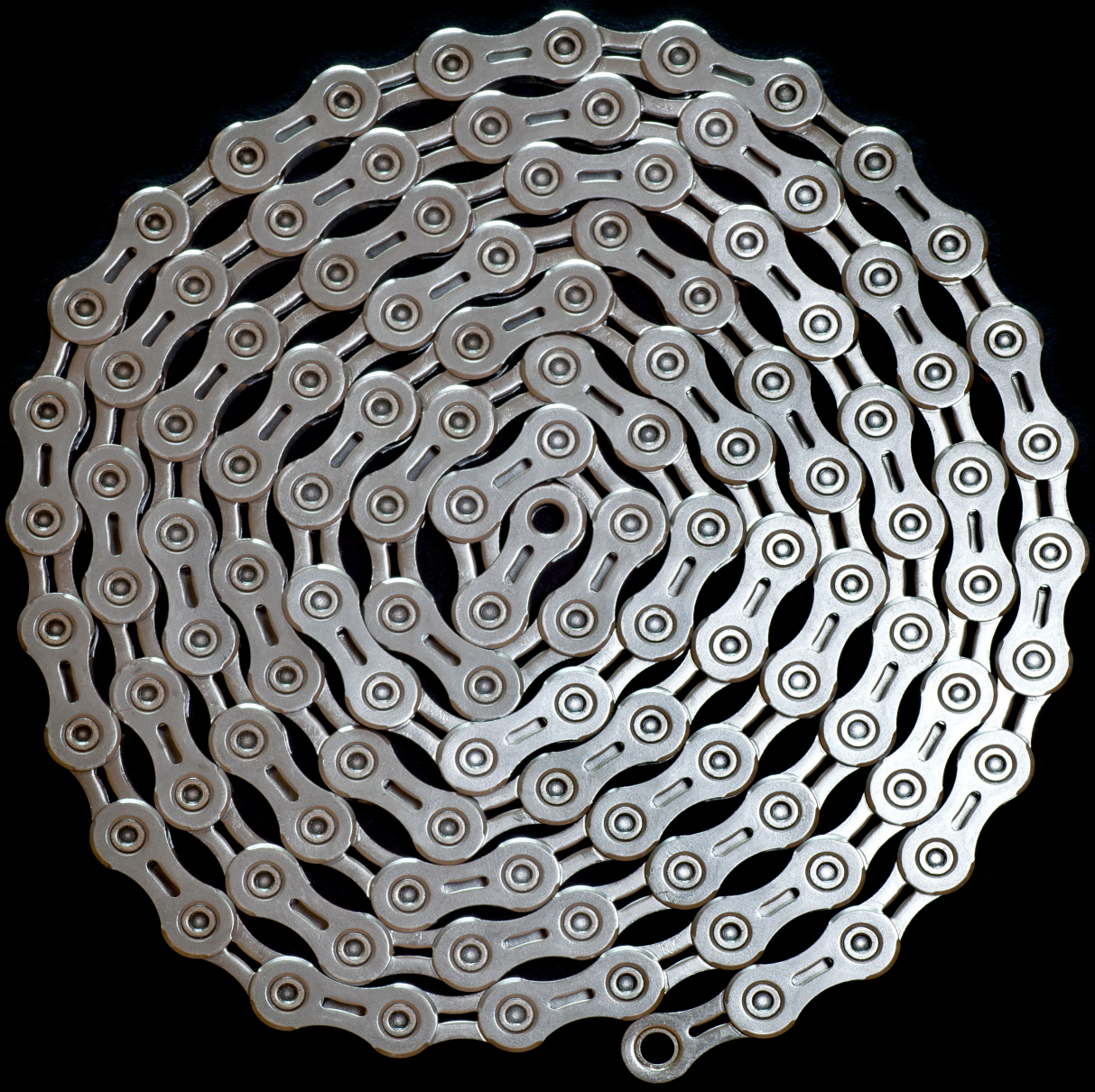
Deloitte.



# Six Control Principles for Financial Services Blockchains

October 2017

This publication, prepared during the summer months of 2017 by the Deloitte EMEA Blockchain Lab in Dublin in association with Deloitte Hong Kong and US, explores six control principles essential for blockchain adoption on a global scale:

01. Best Practice – Standard for Blockchain Development
02. Interoperability and System Integration Controls
03. Audit Rules
04. Cybersecurity Controls
05. Enhancement of Traditional ICT Controls
06. Business Continuity Planning

## Authors


**Lory Kehoe**
Director, Deloitte Ireland
T: +353 1 417 2582
E: lkehoe@deloitte.ie

**Eric Piscini**
Principal, Deloitte US
T: +1 404 631 2484
E: episcini@deloitte.com

**Paul Sin**
Partner, Deloitte Hong Kong
T: +852 28526448
E: psin@deloitte.com.hk

**Eoin Connolly**
Technical Architect, Deloitte Ireland
T: +353 1 483 0338
E: econnolly@deloitte.ie


## Special Acknowledgements


**Niamh O'Connell**
Consultant, Deloitte Ireland
E: nioconnell@deloitte.ie

**Guilherme Campos**
Senior Consultant, Deloitte Ireland
E: gucampos@deloitte.pt


## NL Contact


**Jacob Boersma**
Manager, Deloitte Netherlands
E: jboersma@deloitte.nl

# Table of Contents



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 attracted significant attention in the global financial services community.


CUSTOMER SER
SERVICE L
TIME SCALE
FINANCE
BIG DATA
NEW BUSINESS
CUSTOMER SERVICE
NEW INFORMATION
40%
27%

# Best Practice – Standard for Blockchain Development

Since its mention by Satoshi Nakamoto in the 2008 white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System'[1], blockchain technology, also called Distributed Ledger Technology (DLT), has attracted significant attention among 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 paper, we consider three macro factors which we consider essential to the widespread adoption of private DLTs within the financial community in the long term.

These macro factors are[2]:
01. Governance
02. Legal and Regulation
03. 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 essential for all emerging new technologies.[3] 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.

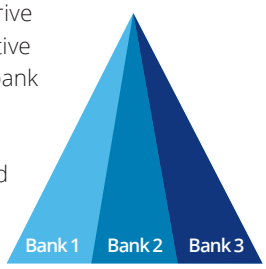
i) A consortium is established by several industry players joining together to form a working group for achieving a common goal.
ii) A joint venture (JV) is a separate, autonomous entity established by two or more companies who share ownership, return, risk and governance.
iii) A statutory organisation (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.

## A 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.

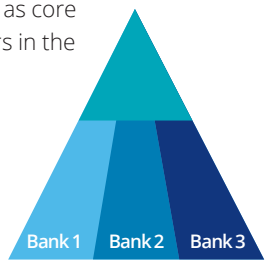
**Participating members contribute resources** to drive common objective forward. Each bank will send a representative to negotiate and make decisions on its behalf.




## B Joint Venture

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

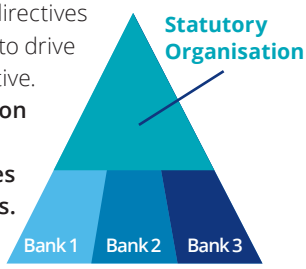
**Jointly funded** by founding members (e.g., banks) as core stakeholders in the Steering Committee.




## C Statutory Organisation

Create a statutory organisation that will operate as a **seperate 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.**



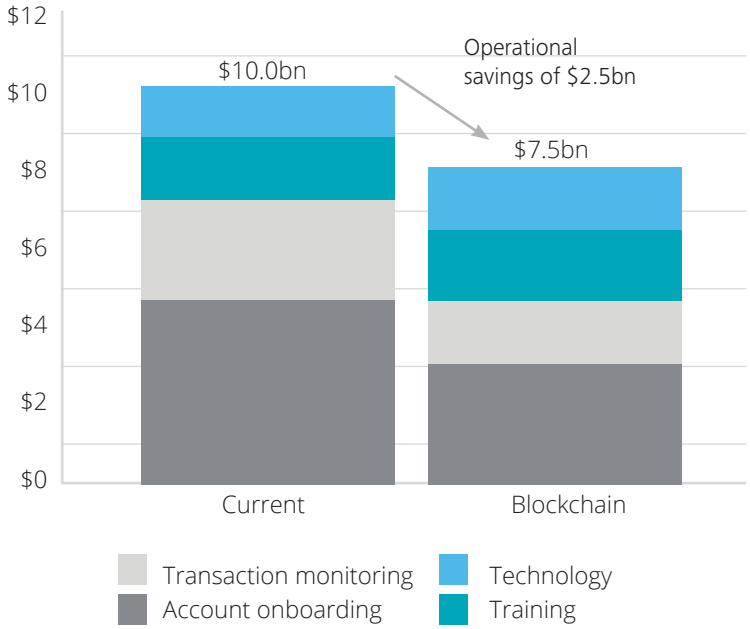

1 Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008
2 De Meijer, Blockchain: How To Make It Operational In Your Company, Nov 2016
3 World Economic Forum Global Risks Report, Jan 2017

### 1.1.1 Consortium

Forming consortia for private DLTs is a popular phenomenon today[4], particularly within the banking sector. Consortium members share set-up 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. For example, a consortium comprising UBS, BNY Mellon and Deutsche Bank recently formed a 'Utility Settlement Coin' to facilitate digital cash settlement.[5]

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 2016 Goldman Sachs report, 'Blockchain: Putting Theory into Practice', 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 $2.5 billion.[6]

While consortium benefits such as shared risk, knowledge and IP are attractive, decision-making can be time-consuming, and holding specific entities and members accountable may sometimes cause internal conflict between members , 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 disagreements occurring in the long term.




Source: Celent, Goldman Sachs Global Investment Research 2016

4 Gilbert & Tobin, Blockchain & Shared Ledgers: The New Age of Consortium, Nov 2016
5 Wiegmann, A, UBS Leads Team of Banks Working on Blockchain Settlement System, Aug 2016
6 Gartner, Gartner's 2016 Hype Cycle For Emerging Technologies Identifies Three Key Trends Organizations Must Track to Gain Competitive Advantage, Jan 2017

### 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 likelihood of internal conflict is lower than with a consortium.[7] 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 would be owned by the JV rather than by the parent entities, and profits would be distributed equally amongst those members with a stake in the JV.

In today's marketplace JVs are being formed between FinTechs and banking institutions. For example, Credit China Fintech entered a $30 million deal with Bitfury which includes setting up a JV focusing on the Chinese market.[8] This JV has since established a working prototype payment system which includes both P2P lender and payment DLT services.

Currently, consortia and partnerships are 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 Organization

In the statutory organisation model, participating members (such as banking institutions) follow the SO's directives and contribute to common objectives. For example, the Monetary Authority of Singapore Electronic Payment System (MEPS+) is an online interbank payment and fund transfer system that is SO-owned and operated.[9] This governance model offers the benefits of transparency and data governance. The regulator provides transparency, has authority over the process for creating standards and monitoring compliance, and ensures that the standards are in line with data privacy regulations (PDPO[10]), 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 the regulators, unless banking institutions agree amongst themselves to use a DLT to store and share information, which may subsequently persuade regulators to adopt the technology.

## 1.2 Legal and Regulation

To maximise effectiveness, DLT commercialisation requires an appropriate legal and regulatory 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 important for driving forward DLT adoption and acceptance.

From a technical and legal viewpoint, lack of clarity about the legal enforceability of smart contracts adds to the risk of implementing DLT within financial institutions. Smart contracts should ideally have the same legal status 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 potential benefits are the 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.

7 Lawless, A, A Guide to a Joint Venture in Ireland, Feb 2010 pp. 6
8 Kastelein, R, Blockchain Startup Bitfury Backed For $30m From Credit China Fintech to Expand To China, Jan 2017
9 Monetary Authority of Singapore, MAS Electronic Payment System, Dec 2006
10 Lovells, H, An Overview of Hong Kong's Personal Data (Privacy) Ordinance: Key Questions For Business, Mar 2014

However, while smart contracts have the potential to serve as legal platforms, a complex two-step process is needed to reach this point. Legislation will have to be enacted to define smart contracts as legal agreements 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 costly. In the absence of pre-emptive legislation or a regulatory decision about the enforceability of smart contracts, it is possible that financial institutions in some jurisdictions may not be able to progress with the implementation 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 does not mean that 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 essential to ensure that all banks agree to 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 the legal and regulatory bodies. Protocols and guidelines need to be agreed and designed. With regard 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 needs to be defined with the DLT protocols, regardless of the governance model. Additionally, data resilience will have to be considered along with data privacy laws (e.g. PDPO), particularly for distributed file systems for documents. Personally identifiable information (PII) will also require special consideration by all parties (e.g. not maintained on the ledger).[11] Lastly, data retention needs to be factored into 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 that speed up the adoption of the technology by financial institutions.

Examples include the 1987 UN EDIFACT standard and the more recent ISO 20022[12] , 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[13], put forward by the national standards authority of Australia, is currently being considered by the International Organization for Standards (ISO). Its focus is on standardising DLTs for interoperability and data interchange among users, applications and systems. Its first official meeting took place in April 2017 in Sydney.

### 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 it 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 develop cross-border standards and agreements, which will be crucial for the expansion of blockchain across all industries. For example, 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).[14]

Forming partnerships or working groups with standard bodies also makes sense for institutions considering whether to establish 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 global standard or code of practice for letters of credit[15] and MT798 from SWIFT deals with the import, export and guarantee of letters of credit.

11 Sponselee, A & Aafjes, N, General Data Projection Regulation, Jan 2017
12 Pupik, J, Explanation: Electronic Data Interchange Standards, March 1997
13 Ryan, P, Proposal for Standardization of Blockchain and Electronic Distributed Ledger Technologies, Feb 2017
14 Gorey, Colm, Deloitte and Irish Funds to Develop regulatory Tech Using Blockchain, Feb 2017
15 Sebban,G UCP 600 – El Mercurio, Sep 2011

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

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 therefore vital that design patterns allow for 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. At some future date it may be necessary to migrate data stored in one contract to another. The contract design should ensure that these data migrations can occur.

**1.3.4 Smart Contract Cyber Security**
Assuming smart contracts are defined as legally binding contracts, new cybersecurity controls will be needed to ensure that the data is stored and held in a secure environment. However, it is important to recognise that most existing cybersecurity standards will also continue to apply. We will go deeper into the topic of cybersecurity controls in chapter 4.

Any code developed for smart contract security must adhere to security best practices and must be reviewed regularly to ensure that newly-discovered security issues are not present in legacy code. Automated tools, if they exist for the blockchain platform, are useful in removing some of the manual effort involved in these reviews.

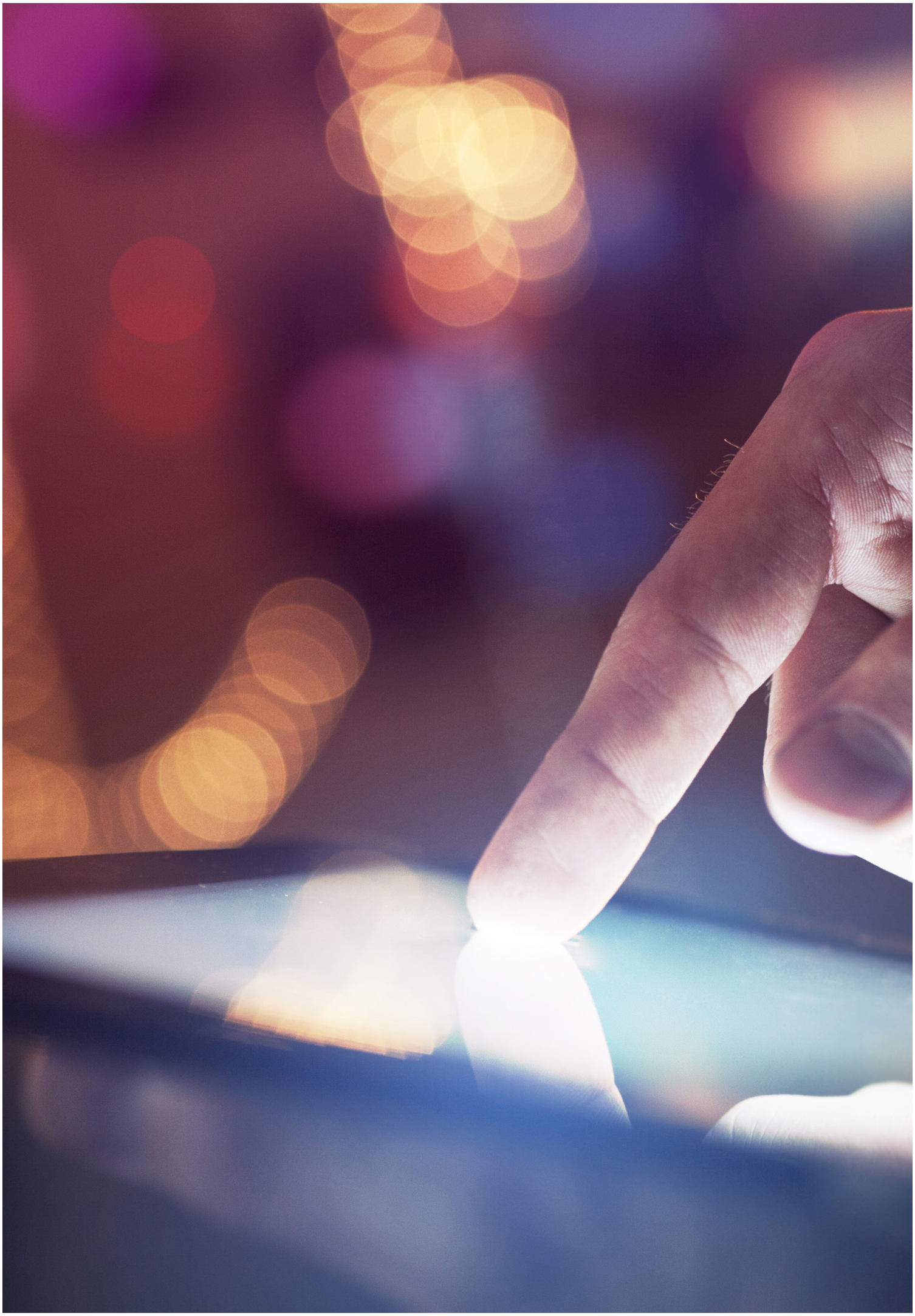
**1.3.5 Smart Contract Interfaces**
Two types of interface need to be considered. The first is the interface between the smart contracts themselves and the data input and output mechanisms to enable data interoperability with other financial systems. Usually this interoperability is delivered by higher-level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

This first type of interface applies to a particular smart contract. The second type of 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 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 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 practice. New standards will also need to be defined for smart contracts, to enable the successful delivery of blockchain solutions into the existing infrastructure of banking and other institutions.

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.



# 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 that all systems are capable of interconnecting and communicating with one another.

### 2.1 Security Considerations

DLT also presents integration challenges with hardware security modules (HSMs) for key storage and generation[16], and security infrastructure such as virtual private networks (VPNs).

Integration challenges with DLTs relate to their security model, which is largely based on PKI (public key infrastructure).[17] Access rights to writing blockchain state data typically require data transactions to be 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 operate without increasing the surface area for attacks, while maintaining the security of a system that potentially contains data from other companies due to the consortium model that is typical of most blockchain arrangements.

### 2.2 Integration with Legacy Systems

DLT solutions within a financial institution are also likely to require integration with legacy financial systems[18] running on a number of different platforms, such as mainframes, web servers, database servers and, more recently, web services or RESTful micro services.[19]

The issues involved in integrating legacy systems are ongoing for financial institutions. For example, an institution may 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 into or extracted from the system.

An issue specifically related to DLTs is the inherently limited data sources that the platform can access, since 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, these data sources 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 pull trusted data automatically from off-chain sources is not a trivial activity, although technical approaches such as the Cryptlets within Microsoft's Project Bletchley blockchain framework[20] 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 complexity 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 Public Key Infrastructure (PKI) specific to DLTs. It is essential that the most secure component (i.e. the tamper-resistant PKI hardware infrastructure) is not compromised by poor security implementation elsewhere, such as unencrypted password databases, unsecured key stores or open Application Programming Interfaces (APIs).

The functional requirements of blockchain implementation could mean integrating a secure

16 Kakavand,H & De Sevres, N, The Blockchain Revolution: An Analysis on Regulation & Technology Related To Distributed Ledger Technologies, 2016
17 Allen, C et al, Decentralized Public Key Infrastructure, Oct 2016
18 De Meijer, Blockchain: How To Make It Operational In Your Company, Nov 2016
19 Williams, C, Is REST Best In A Micro services Architecture?, Dec 2015
20 Grey, M, Microsoft's Blockchain Architecture Overview, Sept 2016

key store service with an internal company user directory, or with an external cloud directory service that can be accessed by all parties within a private consortium. Another approach would be for the assignment of rights to access functionality to be 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 a relatively simple matter. 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 to the blockchain functionality. Most modern programming environments will consume this type of interface[21], which can be used to interact with message queueing systems or service bus applications to provide inter-system operability.

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 or newly-created Enterprise Service Bus (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 mechanisms can be used to integrate disparate DLT systems as easily as integrating DLT systems with more traditional systems. There are additional advantages with blockchain-to-blockchain interfaces, as both endpoints have their interactions logged in an immutable ledger. This simplifies and strengthens the auditing of interactions.

Given the relative lack of complexity in these interface mechanisms, the most important element for a successful integration is the general data architecture of the existing systems and the new DLT. In order 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:

**01. Extract** the data from the legacy system
**02. Transform** it into a format understood by the DLT interfaces
**03. Load** the data into the blockchain

A particular consideration with blockchain data integration is the technological limitations of some platforms. 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, in the case of IPFS , to provide addressing information).

### 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



21 Rodriguez,A, RESTful Web Services: The Basics, Nov 2008

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.

Once blockchain systems have a secure standard interface, they essentially become another enterprise component, albeit with the unique properties possessed by DLT systems.


Monthly results
1000
900
800
700
600
325
838
338
580
472
896
471
489
662
774
mars
avr.
mai
juin
juil.
août
sept.
oct.

# Audit Rules

Will Bible, partner at Deloitte, argues that it is only a matter of time before clients start moving portions of their businesses on to a blockchain-based infrastructure.[22] The existence of DLTs will impact how financial audits are conducted. Blockchains will not automate audits entirely and will not make the role of the auditor obsolete, but rather it will change some of the processes. 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 statements and systems today. Although financial data is stored on an online repository, off-chain records upstream and downstream from the on-chain transactions will also need to be audited. In 2017, Deloitte released the findings of their investigation into applying professional auditing and assurance standards to private blockchain protocols and applications, 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.[23]

### 3.1 The Immutable Record

Data stored on a blockchain is 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 activities, since a blockchain is 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 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 the proper accounting treatment of transactions and factors determining the fair market value of digital or physical assets. It is also important to note that information on the blockchain may be insufficient to determine the appropriate presentation and disclosures within the financial statements. 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 may 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 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 may 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?
- What processes should be followed 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?

22,23 Das, S, Big Four Giant Deloitte Complete Successful Blockchain Audit, Feb 2017

Improperly designed and implemented smart contracts can expose the system to security vulnerabilities. This happened for example 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.[24] As smart contract vulnerabilities may expose a system to the risk of unauthorised access to the data record, security audits and reviews of the code audit rule base 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 be a critical activity when auditing clients with blockchain implementations.

### 3.3 Technical Controls

The existence of a blockchain will 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.[25] Typical controls that 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 relating to the information security policy that an entity would need to address.
- HR security controls. These are the protocols to ensure that access to the blockchain system is updated when employees leave, or change role, within the organisation.
- Asset management controls, and developing guidelines to account for ownership of the platform. These may include guidelines to outline the ownership of hardware tokens (used to store signing keys) and laptops with security certificates installed.
- Access controls. Security roles and restrictions, and the controls for ensuring 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 require 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 apply to the processes around reporting, escalation and response to the breach, and are critical to the safe implementation of DLT.

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

24 Del Castillo, M, The DAO Attacked: Code Issue Leads To $60 Million Ether Left, Jun 2016
25 ISO/IEC 27001, Information Technology: Security Techniques, Information Security Management System Requirements, 2016

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. However, 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 audit 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 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 access and use 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, and some of these systems may 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 that management can deploy more automation, analytics and cognitive capabilities in their processes. Having a large proportion of the data and processing on the DLT could also make possible 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 that auditors work, and they will change the composition of auditing teams, to include specialists in technical blockchain auditing and cybersecurity, however 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 essential to the process.

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.


0005 -4.25%
0003 -10.04%
0001 -10.00%
0003 -14.29%
0005 -12.50%

# 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 may 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 sign interactions digitally, encrypt and decrypt data, and send or receive tokens representing an asset. The security of keys is critical. The ENISA paper 'Distributed Ledger Technology & Cybersecurity' states that: "Stringent policies and procedures must be followed when managing keys, including people, processes and technology". [26]

Breaches involving theft or unauthorised control of these keys can have severe ramifications for a platform using DLT. 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.[27] Later in this chapter, we shall consider 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 in relation 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 (possibly 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 using just 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 are considerably more difficult on a public blockchain, as the attacker must overpower tens of thousands of nodes of specialist hardware. This would require a large hardware and power outlay equivalent to Ireland's total power consumption.[28]

26 Enisa, Distributed Ledger Technology & Cybersecurity- Improving Information Security in the Financial Sector, Jan 2017
27 Verizon, 2014 Data Breach Investigations Report, 2014
28 O'Dwyer & Malone,D, Bitcoin Mining and It's Energy Footprint, Jun 2014

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 put the entire system at risk. Consequently, with permissioned blockchain implementations peers should operate 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 a given number of 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 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 may affect the privacy of data globally. Consequently, developments in this field should be monitored and the cryptographic components of systems should be reviewed regularly to ensure that they remain secure and are not compromised by technological advances.

### 4.2 Smart Contracts

Smart contracts bring their own cybersecurity risks. While a blockchain platform with a Turing-complete smart contract language has enormous capabilities, it also exposes a large security surface area for attackers to exploit (as in the DAO example, referred to 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 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 the code performs its expected functions and is free from known security risks.

Smart contracts are code running on a shared platform, accessed by all parties. Changes to this code affect all entities participating in the chain. When deploying new or updated smart 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[29]) reduce the risk of security holes introduced by non-standard implementations of platform functionality.

29 Frozeman, ERC: Token Standard, Nov 2015

### 4.3 Control Standards

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

The Center for Internet Security Controls[30] include the following:

- CSC1: Inventory of Authorised and Unauthorised Devices
- CSC2: Inventory of Authorised and Unauthorised Software
- CSC3: Secure Configurations for Hardware And Software on Mobile Devices, Laptops, Workstations and Servers
- CSC4: Continuous Vulnerability Assessment and Remediation
- CSC5: Controlled Use of Administrative Privileges

Source: Center for Internet Security 2017

### 4.4 DLT Cybersecurity Strengths

DLTs that use 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 practice, DLTs are potentially more robust from a cybersecurity perspective than systems ,relying on physical or network security, or which are locked with manually-generated passwords rather than cryptographic private keys.

30 Center For Internet Security, CIS Controls, 2017

# 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.

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

The decentralised nature of DLT calls for a differing approach to 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 be read only by appropriate parties.[32]

### 5.1.2 Authentication and Access Control

DLT user access is provided by a public and private keys pair. These keys are unique, and if lost cannot be recovered. Private data on the blockchain needs to be encrypted with the encryption keys for each organisation, and organisations must possess and secure private encryption keys. This need to protect the security of private keys 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 that continuously send and receive information from the network increase the risk of unauthorised access. It is essential that only authorised users and nodes should be able to perform actions in the system. These parties can be external to the organisation and will need to be monitored accordingly.[34]

## 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 be in agreement. 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.

31, 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
35 Hong Kong Monetary Authority, Supervisory Policy Manual : General Principles for Technology Risk Management, Jul 2003, pp.17

### 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 categorize 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, in cases where 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 a high degree of resilience and this beneficial property of blockchain should be leveraged when creating private networks.


The decentralised nature of DLT calls for a differing approach to the management of ICT controls.

# Business Continuity Planning and Blockchain

Business continuity planning (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 reputational damage and loss of client confidence.

With regard to DLT, 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 of BCP might encompass a wide range of complex technical areas, from key storage and key regeneration in the event of catastrophic data loss to creating new keys when a cyber-crime incident compromises data security.

### 6.1 BCP Plan

BCP exercises must cover all 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, the plan must be updated regularly as new risks emerge.
For example, a breakthrough in quantum computing might 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 on 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 such as 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 the 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. According to Kapersky Lab, the number of users encountering crypto ransomware increased by 18% in 2016, with 2.3 million users affected worldwide.[36] Symantec has stated that 43% of ransomware victims were employees in organisations global.[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, business recovery plans need to deal with issues such as redundancy and avoiding data loss or service outage without increasing the attack surface area and reducing operational security. BCP needs to involve internal security teams, with possible validation from external specialists, to ensure that best practices are adhered to during setup, implementation and testing.

In her paper on Blockchain and T2S[39], Margaret Harwood-Jones wrote: "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."

36 Kaspersky Lab, KSN Report: PC Ransomware in 2014- 2016 – The Evolution of The Threat and It's 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 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 contains a number of nodes, for both redundancy and performance reasons.

#### 6.3.1 Public Blockchain Networks

If the blockchain implementation uses a public blockchain networks such as the Bitcoin or Ethereum network, 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 need to be separated geographically 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 some nodes of the private blockchain on the 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 to ensure that 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 BCP is affected by some specific concerns and complexities around cryptography and cyber-crime. Security specialists, both internal and external, play a vital role in ensuring that processes conform with best practice and keep pace with developments in cryptography. While 'traditional' BCP concerns about data loss are mitigated by the distributed nature of DLT platforms, solutions 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, since blockchain implementations are not yet common, there is an additional risk in being a first-mover. This is because 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.

Deloitte.

Deloitte, a partnership established under the laws of Ireland, is the Ireland member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. Please see About Deloitte to learn more about our global network of member firms.

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with approximately 263,900 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has nearly 3,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients so they can move forward with confidence.