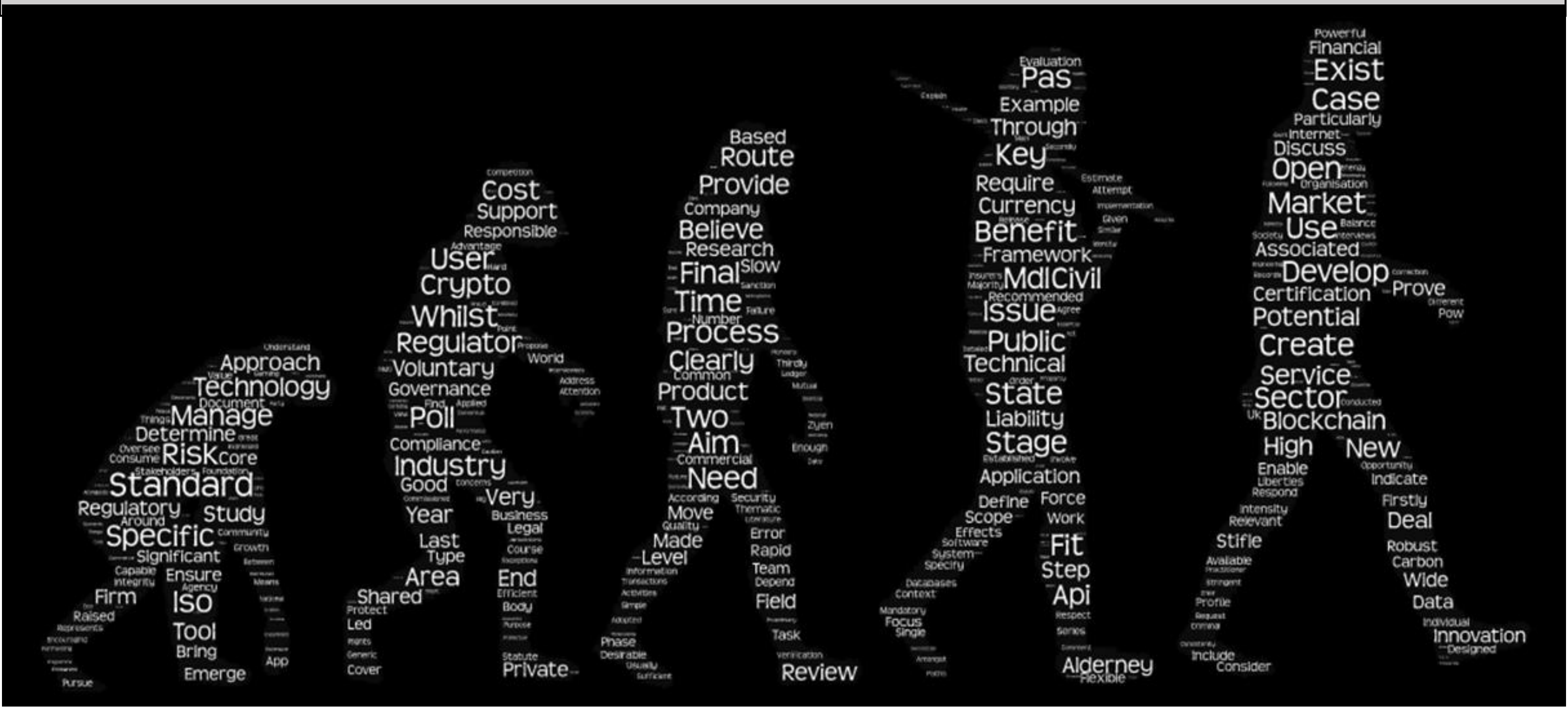
LONG FINANCE

The Missing Links In The Chains?

Mutual Distributed Ledger (aka blockchain) Standards



pwc

CARDANO
FOUNDATION

STATES OF ALDERNEY

November 2016

Contents

Foreword 2

1. Executive Summary 3

2. Background & Methodology 10

3. Mutual Distributed Ledgers (aka blockchains) 12

4. Fitting MDLs Into Existing Regulatory And Standards Frameworks .20

5 Developing New Standards For MDLs 54

6. Findings 59

Acknowledgements 61

APPENDIX A – Sample Existing Standards Applicable To MDLs............63

APPENDIX B – Case Studies Of Cryptocurrency Governance Issues 65

APPENDIX C – Technical Background On MDLs...................................68

Foreword

Long Finance aims to *"improve society's understanding and use of finance over the long-term".* Without doubt, business and technology commentators believe that mutual distributed ledgers (MDLs, aka blockchains) have enormous potential to transform business and finance over the long-term.

The States of Alderney commissioned this study into standards for MDLs because, as regulators for a variety of financial markets, we wanted to improve our understanding of MDLs and how they might be appropriately regulated. We also wanted to understand how voluntary standards markets might interact with regulation. Our theme for MDLs has been 'regulate, use, support', by which we mean "understand how to regulate MDLs", "see where we can use MDLs for regulation itself", and "consider delivering regulatory services that will support appropriate MDL innovation in financial services".

The study concludes, rather pragmatically, that there are many existing technical standards that cover many of the risks of what are, in essence, multi-organisational databases with a super audit trail. However, there are some gaps that standards might address, most notably the governance of the pan-organisational relationships, such as sharing identity information or indemnifying shared information mistakes, where new standards may be necessary.

This report provides an early indication of the path ahead that we may travel from early stage prototypes of MDLs towards a reliable piece of financial services technical architecture.

Bob McDowall
Chairman, Policy and Finance Committee
States of Alderney

1. Executive Summary

Introduction

Mutual distributed ledger (MDL, aka blockchain) technology has captured a great deal of attention. The World Economic Council believes it has "*captured the imaginations, and wallets, of the financial services ecosystem*". SWIFT states that MDLs "*have the potential to bring new opportunities and efficiencies to the financial industry*". The UK's Chief Scientist believes MDLs to be "*powerful, disruptive innovations that could transform the delivery of public and private services*".

As with any new technology, MDLs expose organisations to new risks. Regulators have responsibility for protecting consumers and overseeing the integrity of markets. Regulators respond to risks in two main ways: through the development of specific regulations or by encouraging the establishment of voluntary standards markets.

Objective

The goal of this study was to understand the risks associated with MDLs, examine how MDLs could fit within a regulatory framework, identify aspects of MDLs that would benefit from the development of standards, determine the sectors and services which would most benefit from the application of MDL standards, and assess the development paths that could be used to create standards.

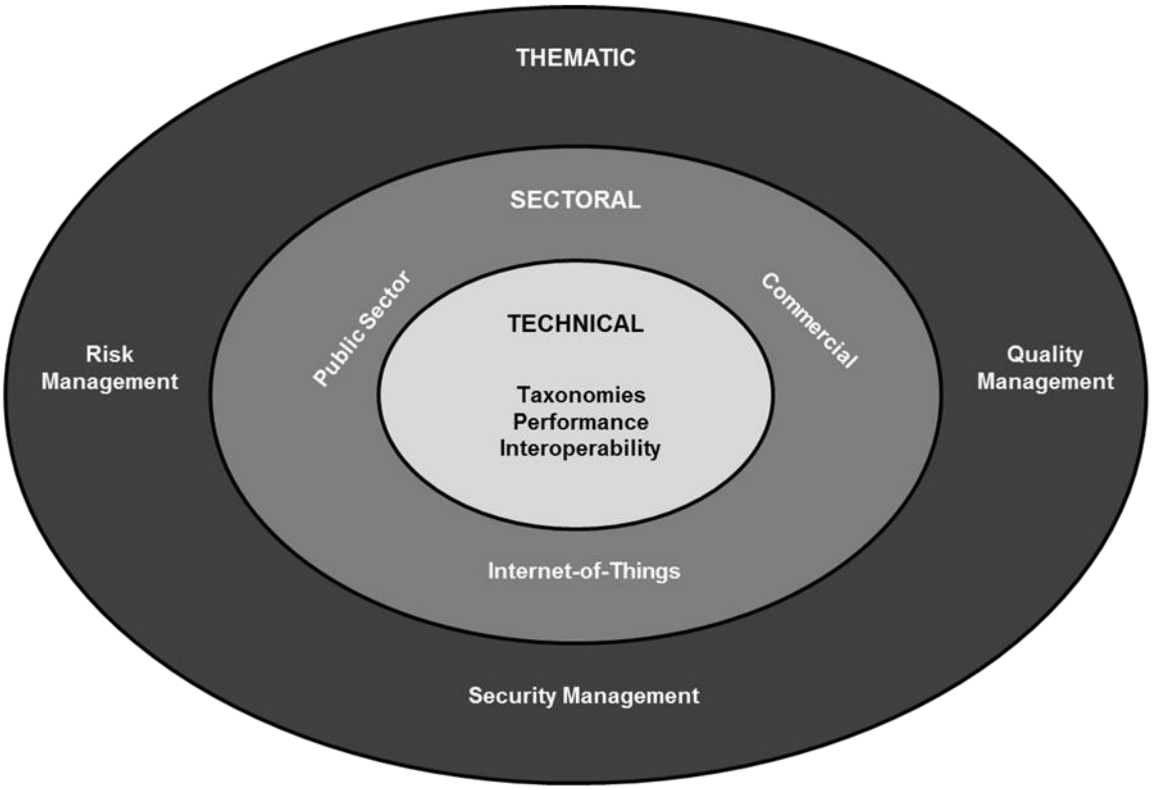
This study aimed to create a dialogue around standards, raising awareness of the need for appropriate standards among developers, users, and regulators. The study was intended to show the range of options for developing standards. In addition to a workshop and a webinar, interviews were conducted with over 60 individuals representing developers, the legal profession, accountancy practices, the financial services industry, regulators and standards agencies. A presentation was also made to the Financial Stability Board at the Bank of England. The results of these discussions shaped the final report.

Risk Profile

MDLs, have proved resilient, having been publically tested in the hostile environment of cryptocurrencies. However, the structures and systems in which blockchain MDLs have been embedded have not proved so robust, and several high profile fraud and theft cases have made headlines (see Appendix B for some examples).

MDLs can be viewed as multi-party databases, and as such they do not exist in isolation - they are there to do something, for somebody, over some period of time. The risks associated with databases are well understood and a wide range of standards have been developed to manage them. However, the shared nature of MDLs will create a different risk profile to traditional databases.

Representation Of The Standards Environment For MDLs



Managing Risk Through Legal Frameworks

Literature review and discussions with insurers, accountancy and legal firms, as well as members of the development and user communities, indicates that, existing legislation (with some minor adjustment) is likely to be sufficient to cover the activities which may be supported by MDLs.

The introduction of new regulations would not be welcomed by the user or developer communities. Attempts to directly address the growth of the cryptocurrency markets, such as the BitLicense introduced by New York State regulators, have raised issues around the cost of compliance, which some interviewees suggested could damage the attractiveness of jurisdictions as locations to do business.

Managing Risks Through Standards

MDL technology is at a very early stage of acceptance and while a number of developers and consortia have proposed products, there are few working examples of non-cryptocurrency applications. The consensus from interviewees was that MDLs would benefit from the development of a voluntary standards market as, not only would the development of a standard enable an efficient and effective framework for organisations to manage risks, they would bring benefits to regulators by establishing a vibrant compliance and verification 'voluntary standards market'.

Managing Risk Through Professional Qualifications

Another approach is to try and control risk by having suitably trained or qualified individuals perform some or all of a regulated or sensitive activity. To date, information technology professional certification has been left to market forces for the most part. Given that MDLs are another form of database, there did not seem to be much appetite from participants in the study for a specialised MDL professional qualification at this time.

Voluntary Standards Markets

A voluntary standards market is "a commercial system in which actual and potential buyers and suppliers of products and services rely on conformity assessments". Conformity assessments are carried out against standards and can consist of self-certification, second party and third party independent verification and certification. Voluntary standards markets are used widely in all industries. Voluntary standards markets bridge unregulated markets and regulated markets.[1]

Technical Standards

[1] Michael Mainelli and Chiara von Gunten, "Backing Market Forces: How To Make Voluntary Standards Markets Work For Financial Services Regulation", BSI, Chartered Institute for Securities & Investment and Long Finance (November 2013). http://www.longfinance.net/publications.html?id=841 (retrieved November 2016).

From the interviews conducted in the course of this research, the consensus is that technical standards dealing with performance and interoperability will emerge naturally. While there is a case to be made for formalising these at a later stage, if formalisation takes place too soon innovation will be stifled and smaller developers may be driven out of the market. Technical standards are recommended at this stage.

Thematic Standards

The development of MDL-specific thematic standards, covering issues such as quality management, security management and risk management are unlikely to be necessary, as existing standards such as ISO 9000 (quality management), ISO27000 (information security management), or ISO 31000 (risk management) are flexible enough to be adapted for use with MDLs.

A small exception to this may be carbon emission standards. Proof-of-work public blockchains such as Bitcoin or Ethereum are energy intensive. While the majority of non-cryptocurrency applications for MDLs are likely to be private data structures, and thus will not require proof-of-work, carbon intensity standards for blockchains may be worth exploring and may open up an opportunity to link cryptocurrencies to carbon markets, such as the EUETS.

Sector-specific MDL Standards

While the significance (probability multiplied by the size of the impact) of risk issues associated with MDLs will vary according to sector-specific use, three issues were consistently rated as having high significance by all participants in this study:

- ♦ **Taxonomies & Performance** – an emerging problem with any new technology going through an explosion of new applications is categorising them and determining how to evaluate whether it does ‘what it says on the tin’;
- ♦ **Data Governance & Liability** - the way in which MDLs are managed and permissioned, particularly with respect to error correction and the arbitration of disputes;
- ♦ **Commercial Governance &Liability** - liability and indemnity for mistakes should be carefully considered when relying on shared information in high risk areas such as payments and identity (e.g. Know-Your-Customer, Anti-Money-Laundering, Sanctions Screening, and Ultimate Beneficial Ownership.

Significant voluntary standards market development could be supported in three areas:

- **Taxonomies & performance standards**: this needs to be an outcome-focused set of definitions and categorisations, i.e. if presented with a MDL can a regulator assess it based on the type of MDL and its performance characteristics, but not how it does what it does;
- **Data governance & liability standards:** given the potential civil liberties risks associated with the use of MDLs in identity systems (a number of interviewees raised the prospect of a panopticon society), and the potential to compile detailed records on individuals by organisations such as financial services companies or governments, it is recommended that standards are developed which specify, *inter alia,* how records on individuals are kept on distributed ledgers, who owns this data, under what circumstances, if any, it may be aggregated into a single MDL, and the procedures for correcting errors and removing data. Given the significance of issues associated with liability, responsibility, and security, for the internet-of-things, e.g. autonomous cars, security systems, telecommunications, it is recommended that particular attention is given to standards for devices;
- **Commercial governance & liability standards**: it is essential that the use of MDLs in commercial transactions does not undermine confidence in the integrity of markets. To this end, particularly in the financial services sector, the development of a standards framework which manages risks associated with governance, liability, identity, responsibility, and compliance is desirable.

Processes For Developing Standards

One of the strengths of voluntary standards is that they exist in a market - users are free to choose the most effective standard which meets their needs. As such, there are three potential routes which can be used to develop standards in this space:

- **International Standards Organisation (ISO)**: In order to pursue this route, it would be necessary to propose a new standard to ISO/IEC JTC 1 the technical committee responsible for Information Technology, or any other relevant committee in the case of other MDL areas. The benefits of this process would include a clearly defined verification and certification route and enhanced credibility for any standards created. Standards Australia has announced (15 September 2016) that it will manage the secretariat of an international technical committee for the development of blockchain standards after ISO approved its proposal for new international blockchain standards[2];

- **National Standards Institutions:** The ANSI, BSI, DIN and other nationally based standards institutes have similar processes for the development of Publically Available Specifications (PAS). A PAS is a document that standardises elements of a product, service or process. PASs can be commissioned by individual companies, trade associations or government departments. The advantage of a PAS is that it is developed in consultation with relevant stakeholders and PAS specifications tend to be less onerous than full ISO standards. If a PAS proves popular it can be developed into an ISO standard;
- **Open process**: The development of a regulator-led, open process, based on the Internet Engineering Task Force (IETF) Request for Comment (RFC) series is an alternative route. While the development of open standards can be resource intensive, the advantage of this approach is that it is led by the practitioner community and can provide a robust product that this tailored to industry needs. Careful consideration needs be given to the establishment of robust, transparent verification and certification processes in order to ensure the credibility of a standard coming from industry.

Summary Of Findings

- Existing regulations are, for the most part, sufficient to oversee the activities which are likely to benefit from MDLs.
- Technical operation standards are not necessary at this stage of the development of MDLs.
- Professional qualifications for developers and operators of MDLs are not yet needed.
- There may be scope to develop a carbon standard for cryptocurrencies.
- Sector specific standards are desirable and would benefit:
  - developers, through enhanced trust and understanding of the technology by users;
  - users, through the creation of a trust framework that manages risk;
  - regulators, by limiting threats to the integrity and reputation of markets.
- Standards would be particularly beneficial in the areas of:
  - taxonomies & performance;
  - data governance & liability;

[2] Standards Australia press release, "Australia To Lead International Blockchain Standards Committee" (15 September 2016) - http://www.standards.org.au/OurOrganisation/News/Documents/Australia%20to%20lead%20international%20blockchain%20standards%20committee.pdf (retrieved 30 October 2016).

  - commercial governance & liability.

- There are a number of routes that can be taken to develop sector specific standards; however, all of them depend on the establishment or use of a robust verification and certification process.

2. Background & Methodology

This study was commissioned by the States of Alderney in May 2016 to look at a voluntary standards market regulatory framework for the use of MDL technology. Alderney understand the value of creating a robust, flexible regulatory framework for enabling electronic commerce. Alderney's experience in eGaming has shown that providing an independent regulatory framework is attractive to many commercial operators. Alderney has embarked on a programme aimed at providing a regulatory framework for the use of MDLs. There are three strands to the programme:

1. Determining the range of potential MDL standards and identifying gaps that need filling;
2. Developing a framework that would be capable of evolution and able to add a 'standards process' to new applications;
3. Supporting a 'voluntary standards market' approach before requiring direct regulation.
   This report represents the first step in this process.

Methodology

This scoping study was developed by a process of interviews with practitioners and other stakeholders, supplemented by a workshop, a webinar and desktop research. The focus of the interviews was to identify stakeholder views on:

- ♦ potential issues and challenges associated with the application of MDLs across a range of sectors;
- ♦ ways that these issues may be addressed by developers, users and regulators.

Interviews were conducted on a semi-structured basis[3], and combined a pre-determined set of open questions with the opportunity to explore particular themes or responses further[4]. Participants were interviewed either in person or

[3] Dalkey, N., & Helmer, O. 1963. *An Experimental Application of the DELPHI Method to the Use of Experts*. Management Science, 9(3), 458–467. http://pubsonline.informs.org/doi/abs/10.1287/mnsc.9.3.458 (retrieved 4 July 2016)

[4] Diamond, I. R., Grant, R. C., Feldman, B. M., Pencharz, P. B., Ling, S. C., Moore, A. M., & Wales, P. W. 2014. *Defining consensus: a systematic review recommends methodologic criteria for reporting of Delphi studies*. Journal of Clinical Epidemiology, 67(4), 401–9. http://www.ncbi.nlm.nih.gov/pubmed/24581294 (retrieved 4 July 2016)

by telephone, and were selected to represent the following groups of stakeholders:

- software developers and suppliers of MDL services;
- regulators;
- standards developers;
- legal professionals;
- accounting professionals;
- financial services professionals;
- wider industries;
- certification and accreditation professionals.

A workshop using "Future Wheels"[5], a structured brainstorming method used to organise thinking about future events, issues, trends, and strategy, was held on 18 July with a dozen participants. The workshop exercise asked participants to focus on three questions:

- What if global standards become mandatory for the use of MDLs in financial services?
- What if global standards become mandatory for the use of MDLs in the internet-of-things?
- What if the IT industry boycotted the use of government imposed standards?

A webinar was held on 22 September to air the results to interviewees and others.[6] Many of the comments and questions influenced this report.

The aim of this study was to be rapid and relevant. No attempt has been made to estimate the potential costs of risks to users or markets, or the potential benefits of voluntary standards to industries or the economy. The high-level process undertaken does not guarantee 'accuracy', but we believe that it provides a good starting point for developing a sense of direction.

[5] J C Glenn (2003), The Millennium Project: Futures Research Methodology V2.0, ISBN: 0-9722051-1-X

[6] Webinar: Intergovernmental Standards for Mutual Distributed Ledgers Discussion Forum, (22 September 2016) - http://www.zyen.com/Presentations/Presentations/Research%20Into%20Inter-Governmental%20Standards%20for%20Mutual%20Distributed%20Ledgers%202016.09.pdf

3. Mutual Distributed Ledgers (aka blockchains)

Characteristics Of MDLs

MDLs securely store transaction records in multiple locations with no central ownership, and so they allow groups of people to validate, record and track transactions across a network of decentralised computer systems. In such a system, everyone shares the ledger, though varying degrees of control, or permissions, are granted which dictate who is allowed access data and who can write new data onto the ledger.

The ledger itself is a distributed data structure held, in part or in its entirety, by each participating computer system. Trust in safeguarding and preservation moves from a central third-party to the technology itself, reducing costs and speeding up transactions. MDLs offer new capabilities for firms to interact with each other. In any transaction where multiple participants exchange data, a shared common view of data eliminates the need to duplicate data entry and to reconcile between multiple individual data-silos. A MDL provides a 'logically central but physically decentral' database, eliminating much inter-firm messaging. This allows more efficient workflow for all parties, without the need for a central authority and without a 'single point of failure' risk.

New, emerging techniques, such as 'smart contracts' (executable code stored in a MDL) and decentralised autonomous organisations (complex sets of code that emulate a business organisation) might, in future permit MDLs to act as automated agents. An example of a smart contract might be a weather derivative contract which automatically makes a payment when a particular group of weather stations record events above a trigger rate.

Box 3.1 The Problem of Trust

If Bob offers to buy a car from Alice, how does Alice know that Bob has the necessary funds? And how does Bob know that Alice owns the car in question and will not deny that he has given her the money and hang onto the car anyway? Traditionally, this issue is solved by using a third party, such as a bank, to verify the exchange.

MDLs offer an alternative. By storing a publically available (but anonymised), indelible ledger of all previous transactions in a string of 'blocks', it is easy to trace who owns what and who has sent what to whom.

However, despite some proponents touting MDLs as a universal panacea or disruptor, it is just a technology. For it to be deployed effectively, businesses must analyse specific uses where it will solve a problem more efficiently and cost effectively than an existing solution, as well as managing risks its use generates as a side effect.

The Advantages Of MDLs

Interviewees consistently highlighted one of the most significant benefits of MDLs as disintermediation. Organisations and individuals use central third parties in many roles in business, especially in financial services. Third parties are used for settlement, as custodians, as payment providers, as poolers of risk. Central third parties perform three roles:

- **Validation**, i.e. confirming the existence of something to be traded and membership of the trading community;
- **Safeguarding**, as in preventing duplicate transactions, i.e. someone selling the same thing twice or 'double-spending';
- **Preserving** by holding the history of transactions to help analysis and oversight, and in the event of disputes.

As a consequence, central third parties often reach the state of 'natural monopolies' and may hold the information they guard to ransom. Because MDLs provide pervasive, persistent, and permanent records without central ownership, they significantly reduce the need for third party functions, thus reducing the costs and time taken to process transactions. In addition, the ability of the community to retain mutual control of the data reduces the 'switching costs' of moving any residual central third party functions to a new central third party.

Cryptocurrency Applications Of MDLs

The most well-known application of MDL technology is as the architecture supporting cryptocurrency transactions. A cryptocurrency is a medium of exchange designed, using certain principles of cryptography, for electronic transfer. Unlike fiat currencies, which are issued by central banks, cryptocurrencies are decentralised and their exchange is disintermediated.

Each Bitcoin transaction is recorded in a MDL referred to as 'the blockchain' (Satoshi Nakamoto referred to it as a 'proof of work chain' in his original 2009 paper[7]). The blockchain is a tool that can verify transactions with minimal third party involvement. The names of buyers and sellers are never revealed – only their Bitcoin wallet addresses. Each wallet address is unique and can't be linked to anyone unless the creator of that specific bitcoin address reveals themselves. The use of MDLs to support cryptocurrency transactions solves the 'trust problem' (see Box 3.1).

There are now thousands of Bitcoin lookalikes, as well as some developments that take the concepts further, e.g. Ethereum with its emphasis on 'smart contracts'.

Examples Of Non-Cryptocurrency Applications Of MDLs

Equally, there has been a great deal of interest in MDLs for use in applications other than cryptocurrencies. In order to understand the reasons for the excitement about this technology's potential, it is useful to consider the definition:

- Mutual – shared in common, or owned by a community, or shared by everyone yet owned by none;
- Distributed – divided among several or many locations;
- Ledger – a sequential record of transactions.

In combination then, a MDL is an immutable, tamper-proof, record of transactions shared in common and stored in multiple locations. A MDL is "a multi-organisational database with a super audit trail" [Mainelli].

[7] Nakamoto, Satoshi (24 May 2009). "*Bitcoin: A Peer-to-Peer Electronic Cash System*" https://bitcoin.org/bitcoin.pdf (Retrieved 15 July 2016)

Databases are critical technologies in modern society. Virtually everywhere there are computers there are databases. However, when more than one organisation attempts to share a common database for commercial purposes, issues with trust, security, and verification often necessitate the use of third party intermediaries. This is particularly true when transactions are high-value or commercially sensitive. MDLs have a number of advantages over central databases as, unlike central databases, they are:

- permanent: once entered into the ledger, records cannot be altered;
- persistent: their distributed, unalterable nature means that the loss of a complete database is almost impossible;
- pervasive: everyone has access to common data and MDLs can replace much inter-organisational messaging.

To date, the principal applications for MDLs have been cryptocurrencies and their use in exchanges and wallets, largely focused around Bitcoin and Ethereum. While there are a large number of developers, businesses and multi-party collaborations working on proof-of-concept applications for MDLs, there are very few examples of MDLs currently running in business environments. During the course of this research, the only 'live' projects identified outside of cryptocurrencies were government timestamping (Alderney with its www.metrognomo.com), clinical trials recording (Z/Yen and the CLEAR project, as well as other private clinical trials recording projects), chain-of-custody & provenance (Everledger), insurance broking (SafeShare), and reinsurance excess-of-loss administration (Blem Information Management).

Potential Uses Of MDLs

A MDL's strength is helping multiple organisations to work together smoothly and share trust and power. If a database application is within a single firm, a MDL is unlikely to displace a traditional central database. To date, applications have focussed around four themes:

- **Transactions** – banking has been abuzz with chatter about MDLs, perhaps overhyping their potential to replace payments. Meanwhile, some quieter areas of financial services, such as insurance and back-office processing, already use MDLs to do such things as confirm multi-party obligations or provide insurance for the sharing economy;
- **Records** – MDLs are ideally suited for timestamping or datalogging. They can be used to lay down long-term records, such as land registry information. They can be used for geostamping, for regulatory reporting, and for archiving.

Universities have been exploring their use for scientific and academic archives for some time. The States of Alderney launched a free timestamping service, MetroGnomo – www.metrognomo.com [disclosure, provided by Z/Yen, which is being used to log a variety of data, not just financial records but also operational records, such as circa 50,000 clinical psychology trials each day for a US regulatory submission and a UK university;

- **Identity** – the ability to store data cryptographically has unleashed a number of approaches to certified documentation meeting data protection principles such as the 'right to be forgotten' and the 'citizen is the data owner'. Since 2007 Estonia has successfully pioneered a universal, national identity scheme using a type of MDL. Firms such as PwC have demonstrated MDLs that can help exchange anti-money-laundering applications, health records, and educational records. Similar systems can provide business 'passports', an easily shared certified registry of government information about a company;
- **Internet-of-Things** - perhaps the most significant announcement of 2015 was from IBM and Samsung. They announced their intention to work together on ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry), a MDL for distributed networks of devices. With billions of people on the planet, we may need several tens of billions or even low trillions of ledgers recording internet-of-things transactions in case of disputes.

Potential Risks Associated With MDLs

While the technology underlying MDLs is robust, having been publically tested in the crucible of digital currencies, there are a number of risks[8] which must be addressed if widespread adoption is to become the norm in high sensitivity sectors such as financial services. These risk areas include:

- **Taxonomies:** The terminology for MDLs is fluid. 'Blockchain' as a term dates to 2012, 'permissioned versus unpermissioned' ledgers to 2015. This is a natural state for newly adopted technology, but how is a bank or a regulator to react to a fintech firm who approaches them and says their work is based on a MDL or blockchain? More work needs to be done on helping people develop common, standardised language to understand what they are talking about;
- **Performance:** Established technologies fit neatly into categories and their performance criteria are well known. With MDLs this is not the case. How secure it it? What is its validation mechanism? How many transactions can it handle per second? What is its energy consumption? What are its throughput

[8] ESMA 2016 *Discussion Paper The Distributed Ledger Technology Applied to Securities Markets*

rates? How public is it? Is it compatible with legacy systems? What interoperability characteristics does it have?

- **Compliance:** The legality and enforceability of the records or code kept on MDLs, or the inclusion of personal data on a MDL need to be carefully considered. Differences in financial and company laws across jurisdictions mean that supervising a MDL 'network' might be considerably more complex than supervising central market infrastructures. Different nodes may be established in different jurisdictions and subject to different privacy, completion, insolvency and other requirements;
- **Liability & Responsibility:** Protecting the participants in a MDL from joint liability is one important consideration, as is indemnity for mistakes. The risk is increased when relying on joint information, and information sharing structures for areas such as Know-Your-Customer, Anti-Money-Laundering, Sanctions Screening, and Ultimate Beneficial Ownership. Determining roles, responsibilities and authority for the management of MDL processes is an important risk management consideration;
- **Security:** Malicious access to a public MDL, for example using a stolen key, could enable a hacker to gain access, not only to the information stored at the point of attack, but to the full breadth of information recorded on the ledgers. There are numerous configurations of public/private, permissioned/un-permissioned, transparent/opaque, read/write, and multiple MDL key structures. Most of the practical work going forward appears to be private-permissioned-opaque structures with keys controlling read/write access. However, these structures reduce the incentives for community participants to keep the entire ledger as they are unable to access most of it. This in turn creates opportunities for community managers with reduced abilities to exploit natural monopolies;
- **Governance:** MDLs need to evolve and 'evolution' is more difficult because of their 'permanence'. Due to the persistence of data in MDLs, correcting transaction or data errors may be difficult unless a single entity is authorised to promote changes across all nodes. This 'inability to evolve' has already resulted in Bitcoin having problems upgrading to meet requirements and Ethereum having to resort to 'tyranny of the majority' to overturn its own 'smart contract' rules in order to reverse a hack. While Bitcoin has virtually no governance structure, and Ethereum has tried a 'light' foundation structure, most commercial MDLs will require stronger governance structures. These structures need guidelines to help evaluate their appropriateness and effectiveness;
- **Transparency & Reporting:** MDLs could add complexity to risk management and oversight in securities markets. While the use of MDLs should in principle

enhance transparency and the traceability of transactions particularly in securities markets, the encryption of the information could make it harder to disentangle and process the identity of buyers and sellers. XML data standards, helping to ensure consistency across MDLs of data structures and interpretation, as well as standing data standards for codes and indices, are not just MDL issues, but the increased interworking of mutual processes heightens their importance;

- ♦ **Interoperability:** This has probably been the most commonly stated objective of MDL standards but, in truth, has been the least important issue for participants in this study. MDLs are, in most respects, flat files. Interoperability for a competent programmer is straightforward. That said, by 'interoperability' many people implicitly include the XML consistency issues above.

Discussion with practitioners confirmed these risks as relevant to non-cryptocurrency applications of MDLs and further ranked them by risk significance (*likelihood of impact* multiplied by the *magnitude of the impact*) as follows.

Table 3.1 Ranking Of Potential Risks For Organisations Adopting MDLs

Issue	**Description**	**Significance**
Governance	Due to the persistence of data in MDLs, correcting errors may be difficult unless a single entity is authorised to promote changes across all nodes. Requiring the need for trusted third parties- thus potentially negating one of the principal benefits of MDLs.	**High**
Liability & Responsibility	Joint liability and indemnity for mistakes should be carefully considered when relying on shared information in high risk areas such as Know-Your-Customer, Anti-Money-Laundering, Sanctions Screening, and Ultimate-Beneficial-Ownership.	**High**
Compliance	The legality and enforceability of the records or code kept on MDLs as well as differences in privacy, financial and company laws across jurisdictions may make compliance more complex.	**Medium**
Security	Malicious access to a public MDL, for example using a stolen key, would enable a hacker to gain access, not only to the information stored at the	**Medium**

	point of attack, but to the full breadth of information recorded on the ledgers on some types of MDLs, yet not on others.	
Transparency & Reporting	MDLs could add complexity to risk management and oversight in securities markets if data is encrypted.	**Low**
Interoperability	There are currently no interoperability standards for MDL, thus there are potential barriers for trade unless this is resolved. However, interoperability will be a commercial imperative and is likely to be solved by market forces.	**Low**
Taxonomies	The '*Magic Beans Effect*'- uncertainty around technology labelled as "based on MDL or blockchain technology" by developers.	**Low**
Performance	What are its characteristics? Is it fit for purpose with respect to speed, reliability, security, transparency, etc.?	**Low**

Perceptions of these risks among practitioners have been heightened by high-profile thefts of digital currencies (see Appendix 2), however examination of these cases reveals that the thefts were made possible not because of specific weaknesses in MDLs but by wider system weaknesses, both human and electronic. In particular, risks around liability and responsibility, governance, security, transparency and reporting were inadequately addressed.

In the words of an accountant: "*MDLs are complex and the technology is difficult to understand. Most people will not be able to grasp what has failed; they will just believe that the technology as a whole is risky and not fit for purpose*."

4. Fitting MDLs Into Existing Regulatory And Standards Frameworks

This section attempts to structure a largely unstructured field, the intersection of a number of control structures used by society. The following table is overly simplistic, but may help readers distinguish regulations from standards:

Table 4.1 – Standards Versus Regulation

System Role	**Standards**	**Regulations**
Input	Standard	Law
Process	Community negotiation	Interpretations & Guidance
Output	Conformity	Compliance
Feedforward	Price & Quality	Legislation
Feedback	Price & Quality & Reputation	Incidents & Public Opinion
Monitoring	Certification Agency – Inspection Within A Competitive Market Framework	Regulator - Supervision
Governance	Accreditation Agency – Auditing Certifiers Within A Market Framework	Regulator - Legal System

Regulations are rules that derive their authority from legislation. While legislation establishes the general “laws of the land,” regulations provide the specific ways in which those laws are interpreted and applied. Regulations are enforced by regulatory agencies mandated by sovereign Governments to carry out the purpose or provisions of legislation. The role that regulators play in markets is outlined in Box 4.1.

Box 4.1 Role Of The Regulator

Introducing Competition

- Buyers have access to alternative sellers at prices they are willing to pay;
- Sellers have access to buyers without undue hindrance from other firms;
- Market price is determined by the interaction of consumers and firms;
- Differences in prices generally reflect differences in cost or product quality.

Protecting Market Integrity

- Preventing market abuse;
- Avoiding the creation of systemic risk;
- Preventing fraud and financial crime.

Other Roles

- Implementation of jurisdictional policy (e.g. consumer and environmental protection, animal welfare data protection, workers' rights, environmental protection, health and safety);
- Providing information about the market via supervisory or trade reporting.

Regulation is developed as a response to perceived risk. Regulation has the advantages of providing a consistent, level playing field for businesses, providing certainty, and protecting markets and consumers. However, regulation does have a number of disadvantages:

- Regulatory compliance is expensive and the costs are particularly heavy for small businesses as the fixed costs of adhering to rules can be spread out over more revenue in large firms than in small ones;
- Regulations can disadvantage domestic businesses against foreign competition which is not required to comply with particular regulation in its home jurisdiction or, *vice versa*, impede free trade;
- Regulation can be subject to political uncertainty or developed with an incomplete knowledge of markets and processes. This can stifle innovation and growth;

- New regulations can have unintended, unwanted consequences, particularly if they significantly alter market incentives.

MDL regulation could get complex swiftly. As the technology is about communication globally, regulators from numerous areas could become involved. In the US, this could be the Federal Trade Commission (commerce), the Federal Communications Commission (communications and advertising), Food & Drug Administration (clinical trials), SEC/CFTC/OCC/Treasury/state-insurance-boards (finance), just to get started. Globally there are too many potential regulators to enumerate, starting with the World Trade Organisation, global telecoms governance or internet oversight (e.g. ICANN) to voluntary bodies such as the Global Commission on Internet Governance, or emerging areas of regulatory oversight such as cybersecurity. The potential for legal & regulatory conflict is obvious.

A voluntary standards market is "a commercial system in which actual and potential buyers and suppliers of products and services rely on conformity assessments"[9]. Conformity assessments are carried out against standards and can consist of self-certification, second party and third party independent verification and certification. Voluntary standards are typically developed on the basis of consensus of all interested parties, are subject to unrestricted open consultation and undergo systematic review to ensure their continued validity.

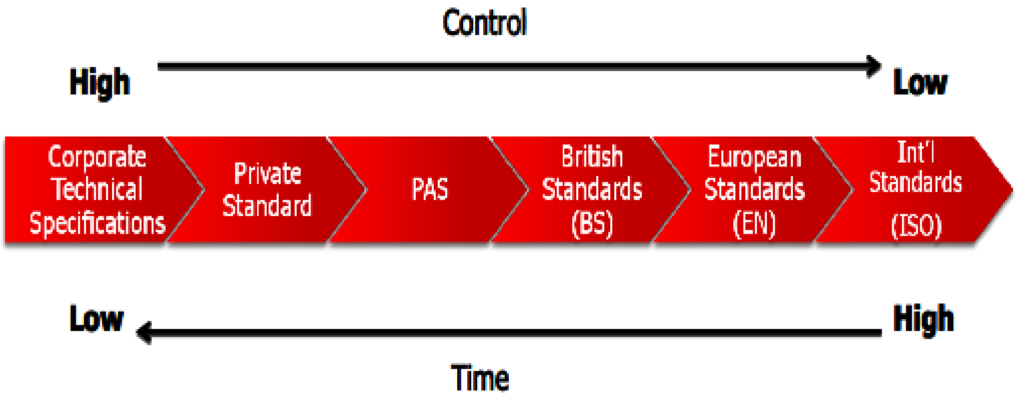
Voluntary standards markets can be distinguished according to their focus[10]:

- **People standards** focus on organisational and individual behavior, values and conduct, and include standards of professional competence and codes of conduct;
- **Product standards** focus on the characteristics and technical specifications of products including design and manufacturing, features, safety, interoperability and materials;
- **Process standards** focus on production or operational processes and include for example data management, quality management systems, disclosure, reporting, risk and resilience management and assessment standards;
- **System standards** provide rules and principles addressing risk at a systemic level including risks related to systemic stability, competition, macroprudential regulation and leverage.

[9] Some standards do not rely on conformity assessments but may be used as guidelines instead, e.g. principle-based standards.

[10] Mainelli, M., & von Gunten, C. 2013.

Figure 4.1 – Types & Evolution Of Standards



[Source: BSI, 2014]

Standardisation is the activity of establishing agreed criteria that provide a reliable basis on which common expectations can be shared regarding specific characteristics of a product (including a service) or a process[11]. Standardisation can be used to support public policy objectives as an alternative to regulation. The standardisation process requires the development of documentation that *"provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that the properties of materials, products, processes and services are fit for their purpose"*[12]. The BSi more prosaically state: *"Standards are the distilled wisdom of people……established by consensus and approved by a recognised body"*[13]

Standards govern the design, operation, manufacture and use of nearly everything that mankind produces. There are standards to protect the environment and human health, standards for materials, components and commercial transactions, there are even standards of acceptable behaviour.

Voluntary standards can evolve over time from a corporate standard – an internal specification or protocol developed and applied within a firm – to publicly available and formal standardisation such as an international standard (ISO)

[11] British Standards Institution 2012. *Principles of PAS Standardisation* http://www.bsigroup.com/LocalFiles/en-GB/PAS/The%20PAS%20Process/BSI-PAS-0-2012-Principles-of-PAS-standardization-UK-EN.pdf (Retrieved 10 July 2016)

[12] International Standards Organisation http://www.iso.org/iso/home/standards.htm (retrieved 10 July 2016)

[13] BSI 2013. Structuring Knowledge: Standards Development Briefing http://www.bsigroup.com/LocalFiles/nl-nl/casestudies/producten/Standards-development-briefing.pdf (retrieved 10 July 2016)

where compliance can be independently assessed through third party verification and audit.

Standards bring benefits by reducing technical barriers to trade and by providing a framework for achieving economies of scale, efficiencies, and interoperability and for improving risk management[14]. They can support public policy objectives and where appropriate offer effective alternatives to regulation. Standards are market-based solutions that enable innovation (e.g. technological standards) and support competition among industry actors where it matters and where it helps clients (e.g. standards granting market access). Competition is good insofar it encourages innovation. Standards should not prevent desirable competition by unnecessarily restricting market access or by discouraging innovation. Competition adds value when it promotes evolution for a period of time. Standards can then emerge over time to address market needs.

How standards are set is a matter of concern. Because the economic and social stakes in standards are so high, standards have major economic and public policy implications. However, despite this governments rarely take a direct role in their development, which can be complex. The process of interpreting laws and creating standards intended to achieve those outcomes often falls to regulators, the governmental agencies that ensure compliance with laws, regulations, and established rules.

However, the development of standards does not fall solely to regulators. Though it is difficult to obtain and define accurate figures, it is estimated that less than 20% of UK standards, and less than 7% of international standards, have their origins in public policy[15]. So most standards are developed by the private sector, often to stay off the need for public policy intervention. “Standards are voluntary in that there is no obligation to apply them or comply with them, except in those few cases where their application is directly demanded by regulatory instruments. They are tools devised for the convenience of those who wish to use them.”

Standards markets are voluntary, typically industry-driven, alternatives to regulation through legislation. Standards aim to increase trust in markets by seeking improved quality, while reducing risks. While regulation is imposed and

[14] Houstoun, K., Milne, A., & Parboteeah, P. 2014. *Preliminary Report on Standards in Global Financial Markets*. (Retrieved 10 July 2016) https://www.swiftinstitute.org/papers/preliminary-report-on-standards-in-global-financial-markets/

[15] Mainelli, M., & von Gunten, C. 2013.

typically controlled by a quota of time or resource, a standard may emerge from market choice. Standards can complement regulation while still supporting competition. Choice in standards means that organisations can choose the standard that best fits their circumstances, balancing the stringency of the standard, the benefits (in risk reduction and reputation) and the costs of implementation.

Standards enable and constrain at the same time. The use of standards requires collective action and the outcomes of these collective initiatives often provide private benefits as well as public benefits. Standards represent the larger architecture within which technological and organisational systems are embedded. The nature of that relationship can have a profound effect on change and innovation within an industry, field, or sector. Where overly rigid standards are set, systems may become over embedded and become prisoners of the standards, thus innovation is stifled. Conversely systems which are under-embedded may not gain the momentum or investment required for wide-spread acceptance, risks may go un-addressed, and, in the event of significant failure, may attract the attention of regulators.

Table 4.2 Comparative Advantages & Disadvantages Of Regulation & Standards

	Positives	Negatives
Regulation	• Necessitates corporate buy-in • Standardisation • Certainty • Level playing field – no free riders • Comparability • Legal certainty	• Knowledge gaps between regulators and industry can result in poorly constructed legislation • One size rarely fits all • Places constraints on innovation • Constrains efficiency and competitiveness • Lack of flexibility in the face of change and complexity
Voluntary Standards	• Flexibility – appropriate for a range of sectors and sizes • Proximity – industry derived standards are efficient and effective • Transparency – standard and compliance is public • Efficient – costs of auditing, verification and accreditation borne by industry • Comparability/competitive advantage	• Credibility of Standard • Management buy-in required • Competition between standards – race to the bottom? • Resource intensive • Sanction free

Types Of Standards

In overly-simplistic terms there are only two types of standard - mandatory standards which have legal sanctions for non-compliance, and voluntary standards which are sanction free (but which can carry economic penalties). The boundaries between them can blur, and the way in which they are developed can vary. A richer look might have four categories:

- **Mandatory standards** require compliance because of a government statute or regulation. Failure to comply with a mandatory standard usually carries a sanction, such as civil or criminal penalties.
- **Closed, proprietary or de facto standards** evolve from a product line or specific vendor (e.g. Microsoft, IBM or Oracle). However, IP owners of de-facto standards may release closed standards to collaborators, or competitors in order to increase the functionality interconnectivity and market share of a product;
- **Open standards** are publicly available, IP free and (may) have been designed through an open process. Open standards are developed collaboratively by organisation, or individuals. They usually emerge in fast moving and rapidly evolving sectors, as their strength lies in their flexibility and ability to absorb and encourage innovation. The RFCs issued by the Internet Engineering Task Force are an excellent example of open standards (see Box 4.2);
- **Voluntary standards can be established by private-sector or NGO bodies** and are available for use by any person or organisation, private or public. The term includes what are **commonly** referred to as "industry standards". A voluntary standard may become mandatory as a result of its use or adoption by a regulatory authorit.

Box 4.2 Internet Engineering Task Force (IETF)

The IETF is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications. The IETF makes voluntary standards that are often adopted by Internet users. These standards take the form of Requests for Comments (RFCs).

The IETF is unusual in that it is completely open source. It is not a corporation and has no board of directors, no members, and no fees. The IETF is made up of volunteers, many of whom meet three times a year to fulfil the IETF mission.

The "Request for Comments" (RFC) document series is the official publication channel for Internet standards documents and other publications of the IESG.

Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force* https://www.ietf.org/tao.html

Well-recognised voluntary standards tend to abide by certain principles, which in turn support their effectiveness and use. While the terminology is evolving, some general principles can be discerned across many voluntary standards markets:

- **Transparency** – outputs such as certifications and grades awarded are published and, ideally, some benchmarking on the degree of pass or fail is given to participants;
- **Openness** – standards should be available to all for inspection, processes for audit, complaints and violations to challenge;
- **Consensus** – development of the standard is an open, structured, inclusive process involving interested stakeholders, conflicts of interest are eliminated and comparators available;
- **Voluntary** – certification agencies compete for audit business – thus encouraging rational interpretation(s) of the standard and controlling cost and quality via reputational risk and competition, and the system can prove exclusion, e.g. certifiers actually mark down organisations that fail to meet the standard;

- **Independence** – accreditation bodies are independent from commercial conformity assessment activities or other undue interests; accreditors can sanction certifiers, for instance ensuring that certification is separate from improvement, e.g. there are no conflicts of interest where firms sell consultancy services to attain a standard alongside certification services;
- **Efficiency** – a functioning market should evolve and improve over time; onerous standards should be simplified; best practices should improve; less time should be spent on checking the obvious as practices become common;
- **Coherence** – there is an authorised, responsible accrediting body for certification agencies that helps to ensure proportionality and consistency; accreditors ensure the separation of standards development from the commercial elements of implementation and review; accreditors regulate the market of standards certifiers; accreditation is probably best left to a sole entity, i.e. non-competitive.

Principles help to clarify and strengthen the concept of international standards as well as to improve their effectiveness. Such principles have also been endorsed by international organisations. WTO's Committee on Technical Barriers to Trade agreed in 2000 on a set of principles concerning transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and developing country interest. In its "European Interoperability Framework for pan-European eGovernment Services", the European Union set out the following criteria for 'openness':

- "the standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision, etc.);
- the standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee or at a nominal fee;
- the intellectual property - i.e. patents possibly present - of (parts of) the standard is made irrevocably available on a royalty-free basis;
- there are no constraints on the re-use of the standard."

Voluntary standards focus on different things. For this research project, we distinguish among People, Product, Process, and Systems standards:

- People standards may be defined as standards focusing on people behaviour and qualifications, such as training and professional qualifications and codes of conduct;

- Product standards are widely used and focus on the characteristics or specifications of products including design, size, weight, safety, environmental performance, interoperability and materials;
- Process standards focus on production processes and can be introduced for different reasons: to address how goods are produced, to improve production process efficiencies or to address externalities (e.g. pollution standards). Management system standards are 'process' standards;
- System standards constitute a different type of standards particularly relevant to the financial services industry in that they provide rules and principles addressing risk at a systemic level including risks related to systemic stability, competition, macroprudential regulation, and leverage.

Value standards codify acceptable behaviour for organisations or individuals in a position of responsibility. There are three types of value standard:

- set by organisations and are used to set standards of expected and acceptable behaviour for staff. These carry sanction for breaches which include formal disciplinary action and dismissal;
- set by regulators in response to public policy imperatives. They are supported by legislation which carries sanction, and clearly defined liability for breaches;
- by communities of interest, such as groups of professionals or companies in a commercial relationship, these carry sanction for breaches, determined in an agreed process by a governing body, which may include exclusion from the group.

Professional standards govern the behaviour of practitioners across a variety of professions. It often takes the form of an institute or professional body controlling a licence to practise or to operate, e.g. the British Medical Association, Law Society, Institute of Chartered Accountants in England & Wales, or Royal Institute of British Architects. Currently, few, if any, professionals standards target the financial technology sector, so any developer or firm can produce financial technology software, despite having only informal knowledge of the frameworks that financial service operate in.

Does MDL Technology Require New Regulation?

In his report on MDLs, Sir Mark Walport states that "*distributed ledger systems differ from the conventional financial system in that they are ruled by technical code rather than legal code. One advantage of this is that compliance costs are* *low: participants need only use a compliant software package to issue transactions*."[16]

Certainly, this is partially true in the case of cryptocurrencies where the codes for "mining" and the code for recording transactions, via distributed ledgers, have proved resilient. However, as demonstrated in Appendix 2, this has not protected customers from fraud, embezzlement and theft.

The New York BitLicense was developed as a response to these perceived risks. The licence, issued by New York State Department of Financial Services, became a requirement in August 2015. Individuals or organisations that are located, have a place of business, or are conducting business in the State of New York are covered by the regulations[17] The aim of the license is to provide a framework that allows digital-currency firms to build their services, while protecting consumers through requirements such as anti-money laundering compliance and cybersecurity guidelines

There is some of criticism from industry practitioners that the regulatory landscape in the United States is becoming an increasingly hostile environment for cryptocurrencies. Start-up Bitcoin companies operating across state boundaries require a separate Money Transfer Licence for each state, territory (and the District of Columbia) they are operating in[18] Furthermore, cryptocurrency firms can fall foul of The Financial Crimes Enforcement Network (FinCEN). In May 2015 FinCEN fined Ripple Labs and its subsidiary XRP II a combined $700,000 for failing to register with FinCEN as a money services business (MSB) prior to selling XRP, a digital token used to settle payments on the Ripple network, as well as failing to implement appropriate anti-money laundering (AML) procedures [19].

[16] OCSA 2016. *Distributed ledger technology: beyond block chain Report of the Governments Chief Scientific Advisor*

[17] New York State Department of Financial Services 2015. *"New York Codes, Rules And Regulations, Title 23. Department Of Financial Services, Chapter I. Regulations Of The Superintendent Of Financial Services, Part 200. Virtual Currencies"*

[18] Perez Y 2015. "The Real Cost of Applying for a New York BitLicense" http://www.coindesk.com/real-cost-applying-new-york-bitlicense/ (retrieved 15 August 2016)

[19] Ciccolo J 2015. *An Analysis of the Ripple Labs FinCEN Enforcement Action*, Bitcoin Magazine https://bitcoinmagazine.com/articles/analysis-ripple-labs-fincen-enforcement-action-1432417986 (retrieved 15 August 2016)

Participants indicated that regulatory compliance is becoming a significant barrier to entry for both start-ups and established firms in some jurisdictions. Specific criticisms of the New York BitLicense are that elements of it replicate existing federal regulations and that applying for a New York BitLicense is expensive and time consuming. California state lawmakers have dropped plans for legislation to create a new licence for Bitcoin companies as a result of lobbying by the Bitcoin industry[20].

One developer stated: “While there is a need for regulation in this space, it should be done at a federal level. Otherwise, should each state issue its own licence, the Bitcoin industry would effectively be killed in the US”.

As explained earlier, MDLs have much wider applications than Bitcoin and a focus on digital currencies has the potential to distort the focus of regulators. Insurance is one specific area where MDLs could make great strides yet equally suffer from regulatory lethargy. Historically the insurance sector has been slow to adopt new technology for B2B interaction, and the majority of contract and documentation produced is still largely paper based (though this is beginning to change). Regulators for the insurance sector are geared to deal with paper records. In the US where the insurance markets are regulated on a state-by-state basis, and regulators are at different stages of adopting new technology, their ability to deal with MDLs will vary.

The application of this technology is still in its infancy and few real world applications have entered everyday use. However, discussion with practitioners in the financial services and legal sector indicate that, in applications such as transfers of fiat currency and transactions involving physical assets, bonds, equities or other financial instruments, a mature framework of regulation already exists. The use of MDLs as a tool to expedite transactions should be regarded by regulators in a similar way to the introduction of electronic communication. While there will be an impact on intermediaries, the fundamental processes and regulations covering them will change very little.

The broad consensus among the individuals interviewed in the course of this research is that while general regulation for the use of MDLs in the financial services sector is unlikely to be necessary, in specific cases where the use of trusted third parties is mandated by regulators as part of the transaction process

[20] Clozel L 2015. *Califormia State Legislators Halt Bill to Create BitLicense* American Banker Magazine http://www.americanbanker.com/news/bank-technology/calif-state-legislators-halt-bill-to-create-bitlicense-1090755-1.html (retrieved 15 August 2016)

jurisdictions may have to review regulations to determine whether they are still applicable.

Smart Contracts

The term ‘smart contract’ was coined by Nick Szabo in 1994. He defined a smart contract as “a computerized transaction protocol that executes terms of a contract”.[21] In other words, the terms of a real world legal contract can be compiled into executable computer code that can run on a network and be made partially or fully self-executing, and self-enforcing.

Smart contracts are pieces of executable code stored in MDLs. In some ways, being neither that ‘smart’ nor actual ‘contracts’, it might be better to use a programming term, ‘sprites’. An example of a smart contract might be a deposit product which triggers repayment with interest on a specific date, or a weather insurance contract which makes a payment when a particular weather station records readings above a trigger rate. Promoters of smart contracts speculate about large assemblies of smart contracts forming decentralised autonomous organisations (complex sets of code that emulate a business organisation) that might in future also permit MDLs to act as automated agents.

Practical smart contracts are problematic for a variety of reasons, e.g. stability of data feeds for execution of the code, liquidity and pooling implications for financial contracts, control and revocation, status in law, arbitration/mediation/expert-determination, and security. However, sprites already function on MDLs and have great potential in areas such as data release and escrow to create ‘smart ledgers’.

The concept of smart contracts generates a great deal of interest, particularly in the financial services and insurance sectors, because of the huge efficiencies that could be made through automation and disintermediation. Smart contracts could satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and minimise the need for trusted intermediaries. This would reduce fraud, reduce the need for arbitration, and lower enforcement and other transaction costs.

[21] Szabo N 1994. Smart Contracts http://www.virtualschool.edu/mon/Economics/SmartContracts.html (retrieved 30 July 2016)

However, calling these types of programs 'smart contracts' is somewhat misleading. On a private chain (one which does not require proof-of-work), the assets being transferred have a physical existence off the chain. What is being transacted is a promise committed to code, for some recognised entity to provide something in exchange for that on-chain token. The asset itself is not being moved, just what is written on the database with respect to ownership. So for smart contracts to work there must be a real, legal document which defines the connection between what's written in the chain, and who has the legal right to own that asset[22].

Lawrence Lessig states that "code is law"[23]. He points out that by making a choice about the structure of networks and the applications that run on them, programmers make decisions about the rules under which the systems would be governed. However there are limits to what smart contracts can actually do, as some of the legal principles contained in contractual law are so fundamental to the regulation of economic activity that courts will not enforce otherwise valid contracts if these contract do not comply with more general principles[24].

Most traditional transactions use trusted third parties to validate the trades and assets, safeguard the transactions and preserve the transaction records. Third parties can also enforce arrangements, or enforcement can take place through the legal system. However this route is expensive and time consuming, so there are other means of resolving disputes such as:

- expert determination, where an independent third party makes a final and binding determination in a dispute. this is often used in contracts that require a valuation or technical assessment of who did what how well;
- mediation, a 'without prejudice' process that helps both parties reach a resolution yet often takes into account how a court might interpret the situation;
- arbitration, dispute resolution by a private third party, effectively a private court, often needed in complex international situations or where the parties favour speedy resolution.

[22] Allison I 2016. How are banks actually going to use blockchains and smart contracts? (retrievd 1 September 2016) http://www.ibtimes.co.uk/how-are-banks-actually-going-use-blockchains-smart-contracts-1539789

[23] Lessig L 2006. "Code" Basic Books http://codev2.cc/download+remix/Lessig-Codev2.pdf (retrieved 7 September 2016)

[24] von Haller Gronbaek M 2016. http://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges (retrieved 30 July 2016)

The reasons for such diversity in legal recourse lies in the many ways disputes can arise when transactions go wrong. This is further complicated as proof of execution is not possible under some business models, for example, where execution is dependent on service levels or variable fee rates. This diversity raises several questions around the use of 'smart contracts':

- How do the parties know the code will do what it is supposed to?
- How can it be stopped if something goes wrong?
- How will mediation, arbitration, or expert determination work?

Finally, because smart contracts are essentially closed systems, smart contracts that involve payments requiring the posting of collateral may impose significant restrictions on their users. Locking-up collateral would lead to a serious reduction in the leverage or pooling financial organisations use and would pull liquidity out of markets[25].

The immediate risks of smart contracts, such as provability, can be mitigated by restricting the application of smart contracts to simple tasks and processes, and near-term, or time-limited transactions (thus reducing complexity and providing an opportunity for intervention). For future development, the onus will be on developers to ensure that appropriate data is collected in standardised time and geographical formats in order to ensure that appropriate legal recourse is available should something go wrong.

[25] Mainelli M 2016. Why Smart Contracts Need Shrewder People, http://www.coindesk.com/smart-contracts-need-shrewder-people/ (retrieved 15 September 2016)

Regulation For Identity

A series of record breaking fines levied by regulators (notably in the US and UK) against organisations who have breached anti-money laundering regulations has sharpened companies focus on know-your-customer/anti-money-laundering/ultimate-beneficial-ownership (KYC/AML/UBO/UBO) regulatory issues[26]. MDLs are uniquely useful here in *not* setting up a central third party oligopoly for records and for providing a practical, technical means to comply with EU GDPR (general data protection regulation) requirements for customer control and the 'right to be forgotten'.

Banks are currently required to demonstrate that they have consistent, thorough, and accurate procedures in place which are documented and available for inspection by regulators. MDLs have the potential to provide powerful tools to aid firms in KYC/AML/UBO/UBO compliance, however it is unlikely that new legislation is required to manage their use, provided they meet the due diligence standards required by regulators.

Data Protection And The 'Right to be Forgotten'

How personal data is stored and the circumstances under which it can be shared are the subject of a considerable body of EU GDPR legislation, which has been translated into the domestic laws of member states. These include:

- Directive 2009/136/EC on universal service and users' rights relating to electronic communications networks and services;
- Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws;
- Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters;
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector;
- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

On 1 August 2016 the EU-US Privacy Shield Framework became operational. The Framework was designed by the US Department of Commerce and European

[26] PWC 2013. *Know Your Customer: Quick Reference Guide* https://www.pwc.com/gx/en/financial-services/assets/pwc-kyc-anti-money-laundering-guide-2013.pdf (retrieved 24 August 2016)

Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States[27].

Article 12 of the Directive 95/46/EC the EU gave a legal basis to internet protection for individuals, the so called 'right to be forgotten'. In May 2014, the European Court of Justice ruled against Google in a case brought by a Spanish citizen, who requested the removal of a link to an article in La Vanguardia newspaper about a foreclosure for a debt that he subsequently paid. On its first day of compliance (30 May 2014), Google received in excess of 12,000 requests to have personal details removed from its search engine.[28]

The persistent nature of MDLs will require users to give careful thought as to how compliance with this raft of legislation should be managed, however, the EU-US Privacy Shield Framework was designed to deal with cross jurisdictional data protection issues, such as those likely to encountered by the users of MDL networks, thus it is unlikely that additional legislation is required.

Civil Liberties Issues Associated With MDLs In The Public Sector

MDLs have the potential to transform the public sector- pioneers such as Estonia and Denmark are already demonstrating that not only do MDLs have the capacity to provide efficient, joined-up public services, but the resilience of MDL networks protects them from cyber-assault. Indeed a motivating factor in Estonia's push to become the world's leading digital state is believed to be concern regarding hostile computer activity supposedly originating from Russia. While evidence of the role that MDLs can play in providing secure public services grows, there is concern in some quarters that applications at scale may infringe civil liberties.

[27] European Commission 2016. *EU-U.S. Privacy Shield* http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf (Retrieved 24 August 2016)

[28] Preece C, Clarke R & Curtis J 2015 *Google Right to be Forgotten- Everything you Need to Know* http://www.itpro.co.uk/security/22378/google-right-to-be-forgotten-everything-you-need-to-know (Retrieved 24 August 2016)

Box 4.3 Estonian E-Citizenship And Digital Identity

Following its independence from Russia in 1991, Estonia invested heavily in digital and telecommunications technology. By 1997, 97 per cent of Estonian schools were online, by 2002, the government had built a free Wi-Fi network that covered most of the populated areas, by 2007, it had introduced e-voting and by 2010 all citizens had been issued with chip and pin digital identity cards which enabled them to access a wide variety of public services as well as providing authenticated digital signatures and filing on-line tax returns.

The technology used to support the Estonian digital identity card scheme, (which from August 2015 was made available to non-Estonian Citizens), is DigiDoc, a MDL based family of digital signature and cryptographic computing file formats, utilizing public key infrastructure. It is being commercialised as GuardTime.

A citizen could be issued with a digital identity at birth, which could contain a complete record of their health, marital status, tax records, property, qualifications, criminal convictions, credit rating and voting records (see Box 4.3). Should central banks begin issuing digital Fiat Currency, the trajectory and velocity of money could be tracked. Should the granularity of the data be sufficiently fine, this means that the complete history of a bank note could be determined- who owned it at any one time and what it was spent on. A developer said:

"It is quite chilling - they (the government) could know exactly what you spend your money on, where you are at any moment of the day, who you are talking to and what medication you are taking. All you have to do is link in face recognition software to the CCTV network and you have a total surveillance society."

A mature policy debate is required around these issues, and regulation may be necessary, over and above existing data protection laws, to determine what records on individuals may be kept by public bodies, who owns this data and under what circumstances, if any, it may be combined.

Issues For Regulators

Regulators seeking to oversee activities facilitated by MDLs face a number of challenges. MDLs will enhance the ability of firms to transact internationally without the need for third party intermediaries. Cross-jurisdictional trade, particularly in financial services is commonplace, but the speed with which it may take place using MDLs may add an extra layer of complexity to the job of regulators. The rapidity with which MDLs may become an informal industry standard, once the proof-of-concept stage has been cleared and successful implementations have reached critical mass, may stretch the resources and technical competence of regulators.

Regulators are cognizant that MDLs have potential, yet are in an early stage of development. As such, regulators are under political pressure to ensure that premature or heavy-handed regulation does not kill innovation. Yet the opposite is a caution against a jurisdictional "*race to the bottom*" in an attempt to attract businesses.

Box 4.4 The Views Of The Practitioner Community On Regulation For MDLs

The overwhelming consensus among those interviewed was that the application of MDLs was at a very early stage of development. As such general regulation was undesirable as it would reduce competition and stifle innovation. Furthermore, the views of interviewees indicated that in the vast majority of likely use-cases, existing legislation was sufficient for regulators to manage any risks that might arise.

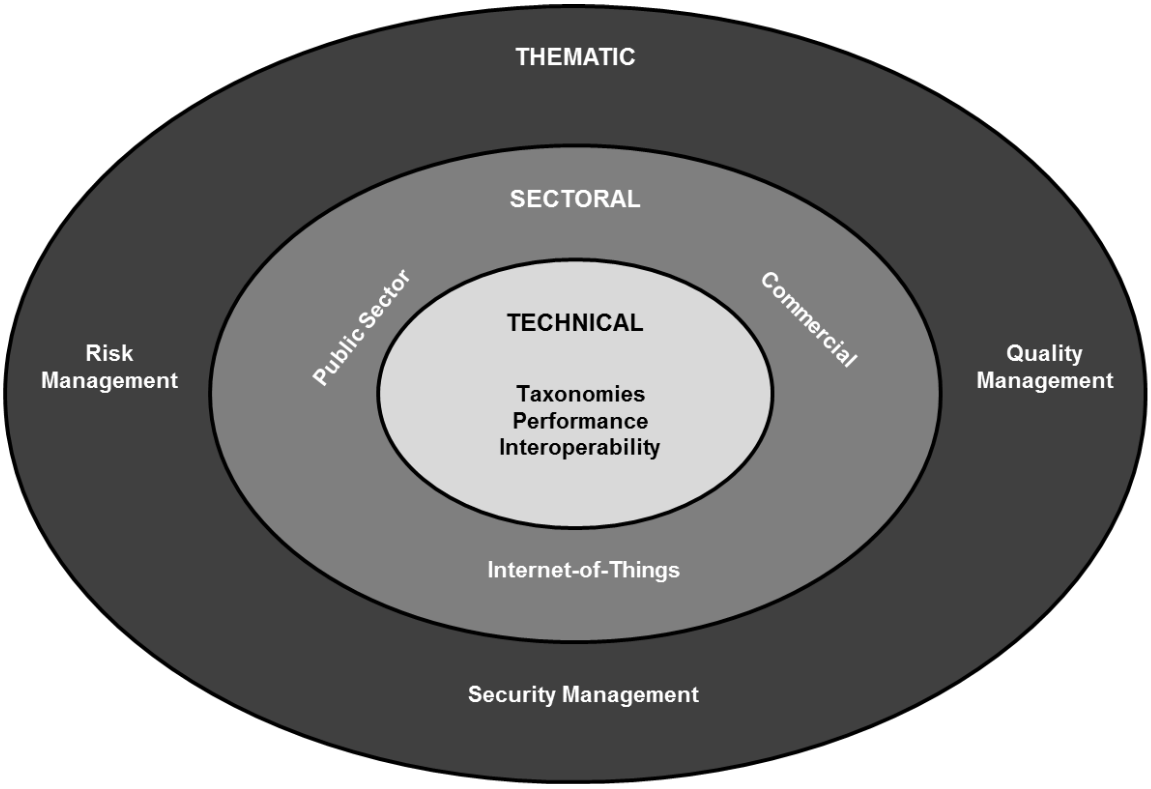
However, several individual did indicate that it was likely that this may change in the wake the first major failure of a MDL-enabled transaction, with one lawyer stating that:

"*Regulation is likely to be shaped by case law arising from litigation. The first big case will shape how MDLs are viewed by regulators and by businesses. There will be a scramble to shut stable doors."*

Does MDL Technology Require New Standards?

Standards can be applied can be applied to MDLs at three levels: Thematic standards can assist in the design and delivery of services in order to ensure that systemic or existential risks are managed. Process specific standards can be applied to particular applications to ensure the quality and constancy of outcomes, and technical standards can be applied to the fundamentals of the technology itself, both in terms of the computer language used and in terms of Performance and Taxonomies.

Figure 4.2 Representation Of The Standards Environment For MDLs



Technical Standards

De Facto Technical Standards include Application Program Interfaces (APIs), a set of routines, protocols, and tools for building software applications, which specify how software components should interact. The release of APIs is particularly common among IT developers, as the release of proprietary code enables the growth of a particular product eco-system. To some degree, not having a public API today is like not having a website in the late 1990s[29] .

APIs are very important as they can define business models. Amazon's release of its APIs means that it is not just an internet retailer, but a retailing platform which is designed to allow easy access to and by other retailers. The success of cryptocurrencies such as Bitcoin and cryptocurrency platforms such as Ethereum is driven by the availability (and ease of use) of their APIs.

[29] Jensen C 2015 "*APIs for Dummies*" (retrieved 10 August 2016) http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WSM14025USEN

[29] Buttle F 1997 *ISO 9000*: *Marketing Motivations and Benefits.* International journal of quality & reliability management

Because of the roles of the regulator in introducing competition and protecting market integrity, de-facto standards are unlikely to make the leap to becoming mandatory. In fact regulators keep a wary eye on the spread of de-facto standards as they can be an indicator of un-healthy market dominance.

Consensus among stakeholders is that de-facto technical standards for MDLs will emerge as they do in many markets, a result of firms trying to gain an advantage. MDL development is in a learning phase, with new players joining the fray with bespoke software solutions. Over time it is likely that certain suites of software will become dominant technologies and technical standards will emerge from their APIs.

Voluntary Technical Standards are flexible enough to apply to MDLs. Among those likely to have a critical role to play are:

- **Computer Languages** - Most web applications have connections to databases and use XML to transfer data from the database to the web application and vice versa. Every major database vendor has proprietary extensions for using XML with relational databases, but they take completely different approaches, and there is no interoperability between them. Developers need to be able to write applications that work for databases from multiple vendors. XQuery and SQL/XML are two standards that use declarative, portable queries to return XML by querying data. In both standards, the XML can have any desired structure, and the queries can be arbitrarily complex.
- **Timestamping** - a trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records) without the possibility that the owner can backdate the timestamps.
  - The RFC 3161 standard (an open standard issued by the IETF) is a baseline time-stamp policy for Time-Stamping Authorities (TSAs) issuing time-stamp tokens.
  - ISO 8601 for Data elements and interchange formats – is the standard for representation of dates and times.
- **Metadata -** manages the meaning or semantics of data to ensure correct and proper use and interpretation of the data by its owners and users. In specific sectors, such as financial services or insurance a number of standards have emerged to manage metadata. These include:

- **ISO 20022** is the Universal financial industry message scheme[30] (which used to be also called "UNIFI") that allows users and developers to represent financial business processes and underlying transactions in a formal but syntax-independent notation.
- **MDDL** The (Financial) Market Data Definition Language has been developed by the Financial Information Services Division (FISD) of the Software and Information Industry Association (SIIA). MDDL is an extensible Markup Language (XML) derived specification, which facilitates the interchange of information about financial instruments used throughout the world financial markets. MDDL helps in mapping all market data into a common language and structure to ease the interchange and processing of multiple complex data sets.

There are formal and informal market standards for many industries, often based around XML, such as Bolero and essDOCS in shipping and logistics, or ACORD in insurance, or FIXML for asset managers and brokers, or FpML for derivatives trading. Voluntary technical standards will dictate interoperability between MDLs and legacy systems, greatly enhancing the attractiveness of the technology and mitigating risks around performance and taxonomies and thus are desirable, in the long-term to enhance uptake of MDLs.

In April of this year, Standards Australia announced that it was pushing for the development of international standards for blockchain that are “compatible with regulations and controls in financial systems to ensure market confidence and consistency in the use of this technology.”[31]

Standards Australia has submitted a formal proposal to the ISO for a new field of technical activity on blockchain and electronic distributed ledger technologies. Currently the scope of the proposal is the “Standardisation of blockchains and distributed ledger technologies to support interoperability and data interchange among users, applications and systems.”

[30] Ali, R., Haldane, A. G., & Nahai-Williamson, P. (2012). *Towards a Common Financial Language*, speech to Securities Industry and Financial Markets Association, NY. Bank of England. (Retrieved 20 August 2016) http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech552.pdf

[31] Standards Australia press release, “Australia To Lead International Blockchain Standards Committee” (15 September 2016) - http://www.standards.org.au/OurOrganisation/News/Documents/Australia%20to%20lead%20international%20blockchain%20standards%20committee.pdf (retrieved 30 October 2016).

Box 4.5 Views Of The Practitioner Community On Technical Standards For MDLs

The interview consensus is that technical standards dealing with performance, taxonomies and interoperability will emerge naturally. While there is a case to be made for formalising these at a later stage, if this takes place too soon, innovation will be stifled and smaller developers will be driven out of the market. We found this comfort with technical evolution proceeding as needed very interesting. One developer stated:

"Dinosaurs (large developers) love standards as they act as fences to keep the small mammals (innovative start-ups) out of their walled gardens"

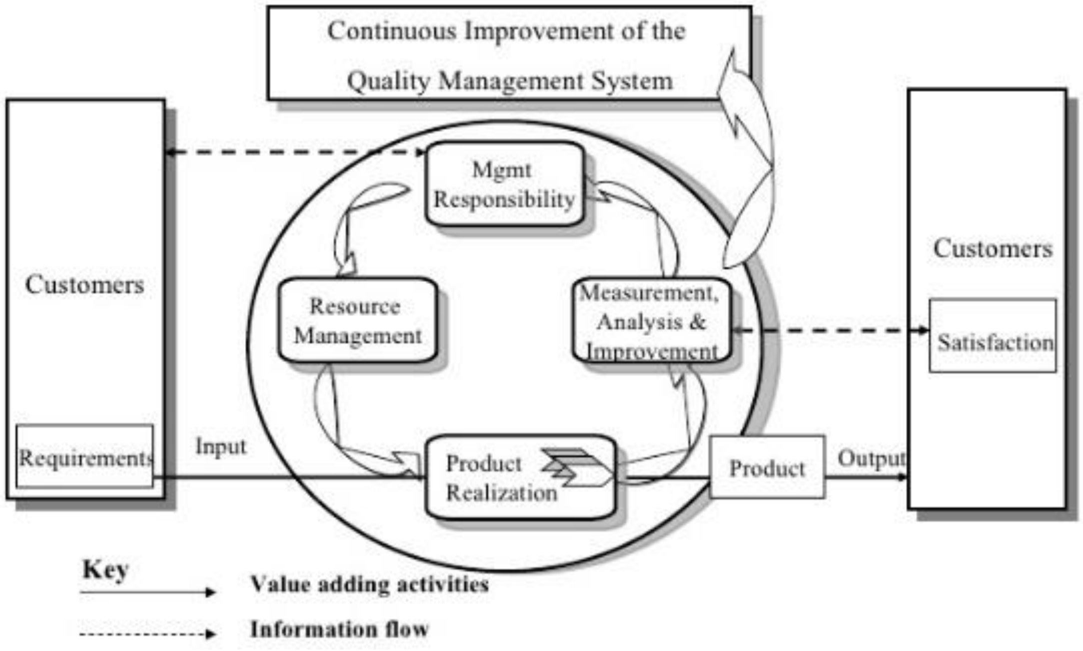
Thematic Standards

Businesses, regardless of sector, face similar challenges with respect to risk, business continuity, security and quality management. In response to these issues, the voluntary standards market has produced a number of products which are designed to standardise the processes used to manage these issues. These include

- ♦ **Quality Management -** The ISO 9000 series of standard is the most widely known and has perhaps had the most impact of the 13,000 standards published by the ISO (ref). ISO 9000 is designed to define, establish, and maintain an effective quality assurance system for manufacturing and service industries, and is grounded on the "conformance to specification" definition of quality[32].

[32] Buttle F 1997. ISO 9000: *Marketing Motivations and Benefits.* International Journal Of Quality & Reliability Management

Figure 4.2 The ISO 9000 process

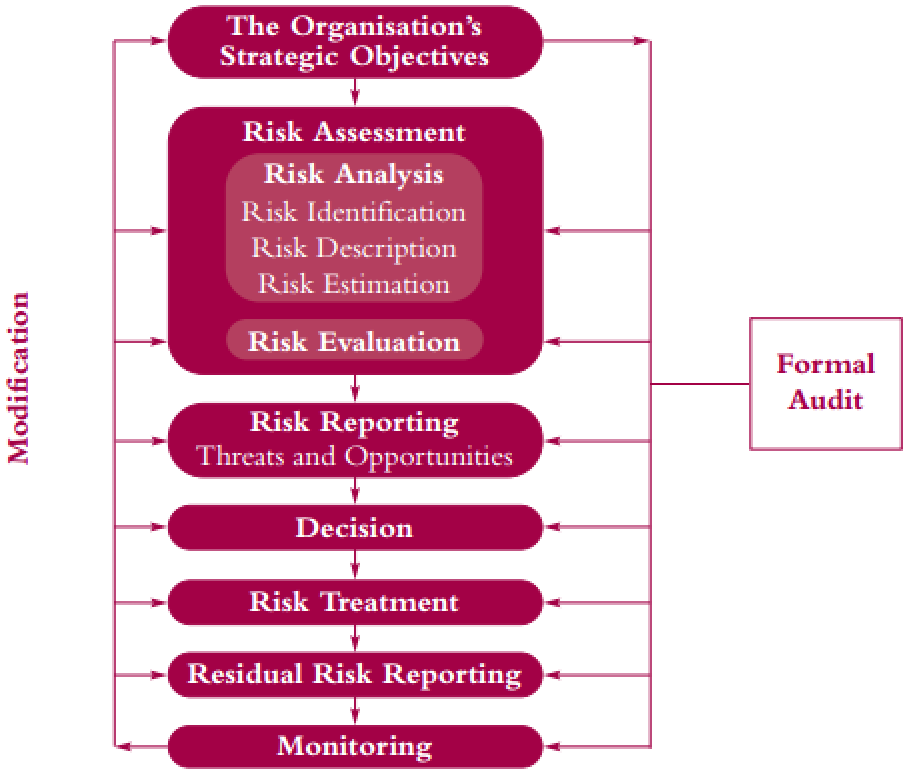


Source: TATA Consultancy Services

♦ **Risk Management -** Worldwide, several standards have been developed to help organisations manage risk systematically and effectively. These standards establish common frameworks, processes and practices. Different standards reflect the motivations and technical focus of their developers, and are appropriate for different organisations and situations however, they share common features. Risk management standards are normally voluntary, although adherence to a standard may be required by regulators. Commonly used standards include:

- **ISO 31000 2009** – Risk Management Principles and Guidelines;
- **A Risk Management Standard** – IRM/Alarm/AIRMIC 2002 – developed in 2002 by the UK’s 3 main risk organisations;
- **ISO/IEC 31010:2009** - Risk Management - Risk Assessment Techniques;
- **COSO 2004** - Enterprise Risk Management - Integrated Framework;
- **OCEG “Red Book” 2.0: 2009** - a Governance, Risk and Compliance Capability Model.

***Figure 4.3 IRM Risk Management standard*[33]**



Source: The Institute of Risk Management

- **Business Continuity-** This is the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident[34]**.**

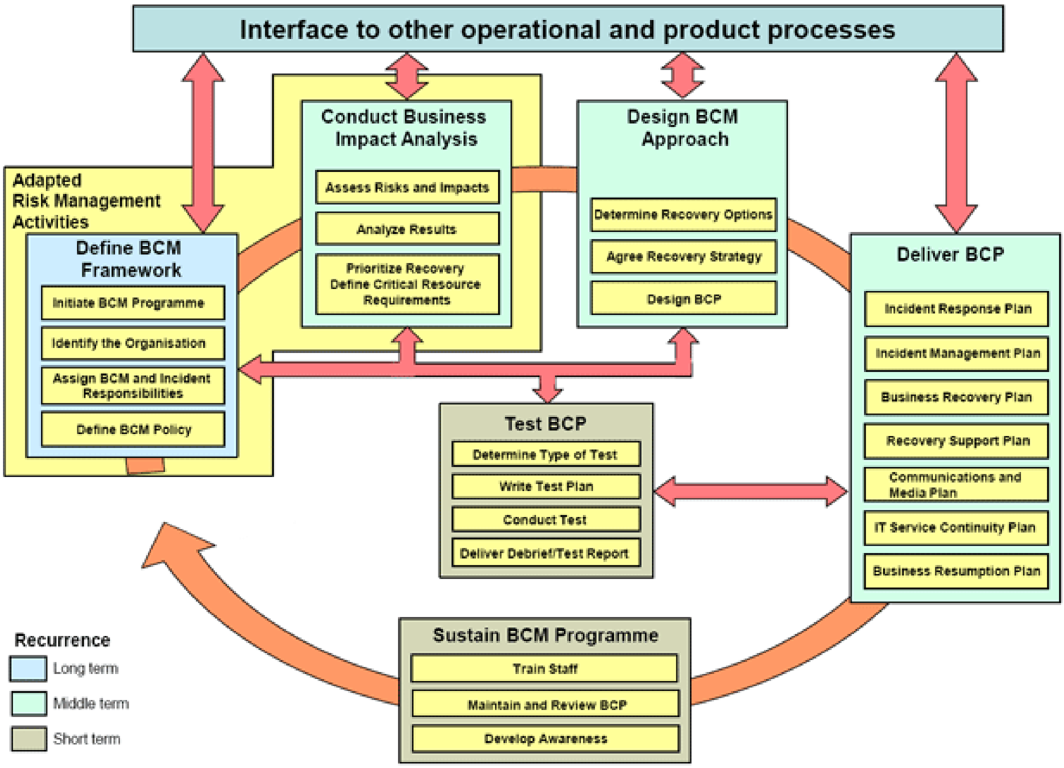
  Globally a number of standards have been produced, these include:

  - **ISO 22301:2012**, which specifies a management system to manage an organisation's business continuity arrangements;
  - **NFPA 1600** standard on Disaster/Emergency Management and Business Continuity Programs, published by the United States National Fire Protection Association;
  - **ANSI/ASIS SPC.1-2009** and **ASIS/BSI BCM.01:2010** published by the American Society for Industrial Security;
  - **AS/NZS 5050** published by Standards Australia.

[33] Risk Management Institute 2002 *A Risk Management Standard* https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf (retrieved 2 September 2016)

[34] International Standards Organisation 2012 ISO 22301:2012 (retrieved 2 September 2016)

Figure 4.4 The Business Continuity Process[35]



Source: European Union Agency for Network and Information Security

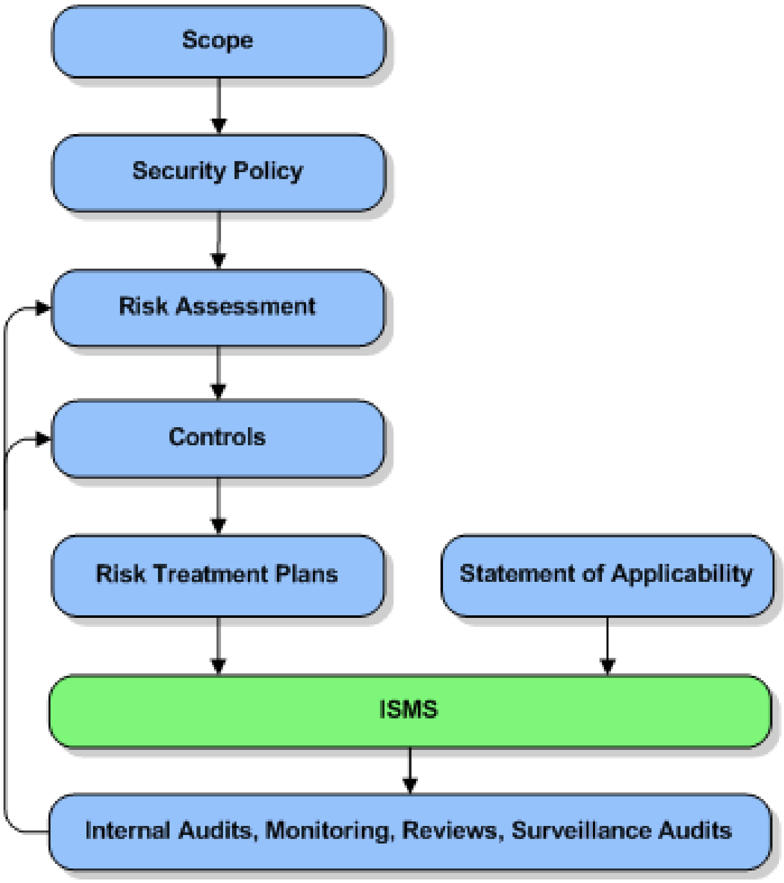
- **Security Management-** Unsurprisingly, given the exponential growth of cybercrime, a number of cyber security standards have been developed over the last few years. These include:
  - **NIST Cybersecurity Framework (NIST CSF)** which is intended to help private sector organisations that provide critical infrastructure with guidance on how to protect it, along with relevant protections for privacy and civil liberties;
  - **RFC 2196** which is memorandum published by Internet Engineering Task Force for developing security policies and procedures for information systems connected on the Internet. It provides a broad overview of information security including network security, incident response, or security policies;
  - **ISA/IEC-62443** which is a series of standards that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner),

[35] EUANIS https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-process (retrieved 31 October 2016)

system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems;

- **ISO/IEC 27001:2013** which is an information security management system (ISMS) standard that formally specifies a management system intended to bring information security under explicit management control. The certification, once obtained lasts three years.

Figure 4.5 The ISO 27001 Process[36]


Scope
Security Policy
Risk Assessment
Controls
Risk Treatment Plans
Statement of Applicability
ISMS
Internal Audits, Monitoring, Reviews, Surveillance Audits

Source: ISO 27001 Resource Centre

There is one aspect of MDLs which may require the development of new thematic standards, and that is carbon intensity. With 'proof-of-work' blockchains a process called 'mining' adds new transaction records to the public ledger of past transactions. This confirms transactions to the rest of the network and ensures that an individual cannot spend the same coin twice.

[36] ISO 27001 Resource Centre http://www.iso-27001.eu/iso-27001-overview.asp (retrieved 31 October 2016)

For Bitcoin and Ethereum mining requires the solving of complex mathematical problems. Each time a transaction takes place, the software underpinning the network reacts by changing a parameter that makes the mathematical problem appropriately difficult to solve. A 2014 paper estimated that the total power used for Bitcoin mining could range from 0.1GW to 10GW. Average Irish electrical energy demand and production is estimated at around 3GW so it is plausible that the energy used by Bitcoin mining is comparable to Irish national energy consumption[37]. If proof-of-work blockchains increase in popularity, they may become a significant contributor to global greenhouse emissions. The development of a carbon standard for MDLs would benefit users as this currently obscure risk may become more significant over coming decades. There may even be scope, in the case of cryptocurrencies, to link proof-of-work to carbon trading schemes and produce a “carbon intensity standard” for cryptocurrencies that links them to a real wold commodity and might reduce market volatility.

Box 4.6 Views on Thematic Standards for MDLs

There was broad agreement among interviewees that thematic standards were specifically designed for their flexibility and should be able to cover the use of MDLs. Note was made that with respect to business continuity the use of MDLs, which are persistent and pervasive, would be a positive advantage. ISO 9000 was held up as a standard which may be particularly compatible with MDLs.

One regulator stated:

“Thematic standards emerged after years of consultation and their proven popularity. Despite the amount of resources required to implement them, their popularity shows that they work. Developing thematic standards just for blockchains or MDLs would be reinventing the wheel.”

Sector-specific Standards

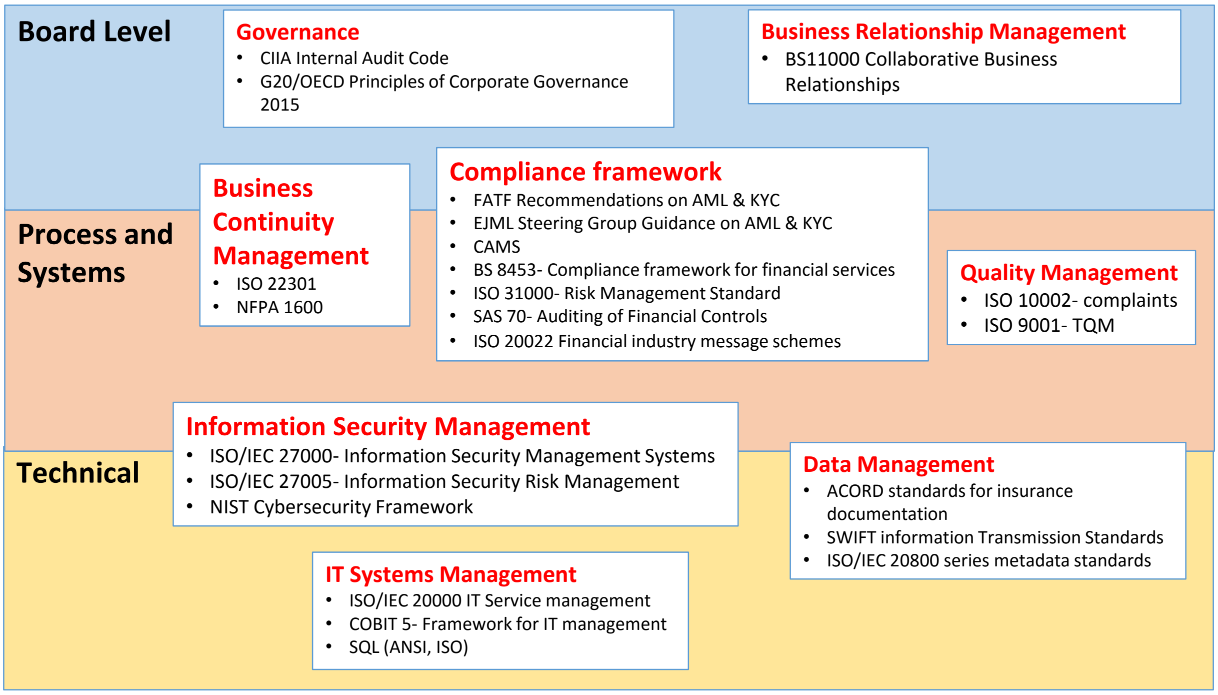
MDLs do not exist in a vacuum. They are built by organisations to perform a particular task over a given period of time. Their ability to do this with minimal

[37] K O’Dwyer and D Malone 2014 Irish Signals & Systems Conference 2014 Bitcoin Mining and its Energy Footprint https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf (Retrieved 10 July 2016)

risk of failure is essential if the technology is to achieve significant market penetration beyond cryptocurrencies.

MDLs are a disruptive technology. The term "disruptive technology" refers to a new technology which has lower cost, but potentially higher performance that existing systems[38]. As discussed earlier, MDLs have a wide variety of applications across a large variety of sectors. In all of these sectors, legacy systems will have evolved, sometimes over decades, to provide secure, reliable services. In certain sectors, such as financial services, the performance of these systems is critical to businesses and any failure may have severe ramifications, particularly with respect to compliance and reputation. The effective management of risks has resulted in a plethora of sector specific standards. Figure 4.6 (below) illustrates some of the standards applicable to the financial services sector.

Figure 4.6 Examples of Standards in the Financial Services Sector



Governance
- CIIA Internal Audit Code
- G20/OECD Principles of Corporate Governance 2015

Business Relationship Management
- BS11000 Collaborative Business Relationships

Business Continuity Management
- ISO 22301
- NFPA 1600

Compliance framework
- FATF Recommendations on AML & KYC
- EJML Steering Group Guidance on AML & KYC
- CAMS
- BS 8453- Compliance framework for financial services
- ISO 31000- Risk Management Standard
- SAS 70- Auditing of Financial Controls
- ISO 20022 Financial industry message schemes

Quality Management
- ISO 10002- complaints
- ISO 9001- TQM

Information Security Management
- ISO/IEC 27000- Information Security Management Systems
- ISO/IEC 27005- Information Security Risk Management
- NIST Cybersecurity Framework

Data Management
- ACORD standards for insurance documentation
- SWIFT information Transmission Standards
- ISO/IEC 20800 series metadata standards

IT Systems Management
- ISO/IEC 20000 IT Service management
- COBIT 5- Framework for IT management
- SQL (ANSI, ISO)

MDLs' ability to substantially reduce the requirement for third party intermediaries in transactions has significant scope to change business processes and thus alter risk profiles. Stakeholders revealed different public and private sector concerns:

[38] Christensen 1997, "*The Innovator's Dilemma; How New Technologies Cause Great Firms to Fail*" Harvard Business School Press

- **Public Sector** - emphasised governance, given the potential civil liberties risks associated with the use of MDLs in the public sector new standards may be required with respect to record keeping on individual citizens with respect to who owns this data, under what circumstances, if any, it may be aggregated into a single distributed ledger, and procedures for correcting errors and removing data;
- **Commercial Sector** - identity, governance, liability, responsibility, and compliance featured prominently, especially as commercial firms wanted to know what were their rights and how they would be recompensed for costs associated with using inaccurate or false shared data.

Identity

Identity standards were almost universally mentioned as requiring closer scrutiny. Identity is a fundamental enabler for innovation and trust in financial services for people, assets, and legal entities. Identity rights precede property rights.

From a development perspective, about 2.4 billion people worldwide lack official identification, of which 1.5 billion are over the age of 14. A large proportion of these are women. They are excluded from market economy property ownership, and frequently free movement, social protection, and empowerment. They cannot ‘prove’ their existence to the satisfaction of society’s registries. Lack of official identification increases remittance costs, corruption, and crime. Insightfully, United Nations Sustainable Development Goal 16 “Peace, Justice And Strong Institutions” contains target 16.9 to “provide legal identity to all, including birth registration, by 2030”.

For financial institutions and high-net-worth individuals (HNWI) in the developed world, there is also a struggle with the plethora of bureaucracy and paperwork involved in KYC/AML/UBO regulation. Onerous KYC/AML/UBO is an obstacle to trade, thus reducing the benefits of comparative advantage and specialisation. Some financial services firms in interviews estimated ‘post sale’ client losses at up to 40%. After prolonged delays due to onerous KYC/AML/UBO processes, numerous customers refuse to proceed further with purchasing ‘sold’ financial services and walk away.

The persistence and pervasiveness of distributed ledgers make them ideal for providing a lifetime records. MDL identity schemes could empower people with personal data storage and management, permission frameworks for access by third parties such as banks insurers or governments, and even distributed reputation ratings. Such applications could reduce financial fraud, costs, and crime, and increase returns, confidence, and security. The concept of never losing data could materially alter the way society views identity, privacy, and security.

A number of firms have started offering MDL based identity verification and business verification services, including Polycoin, which has created software which analyses blockchain transactions to determine if they are suspicious, Credits who are working with the Isle of Man to develop a federated know your customer KYC application and Blockscore are developing a real-time verification and anti-fraud service.[39] In these types of identity systems, there are typically three parties:

- the subject, an individual;
- the certifier, an organisation notarising documents such as a government, legal or accounting firm, a notary, or a credit referencing agency;
- the inquisitor, an organisation conducting KYC/AML/UBO checks on the subject.

For identity MDLs, the key areas of risk are certification (validation of the qualifications of the certifier) and data security (who can access the information). In MDL identity or secure document transmission examples, there are typically at least two distinct MDLs, a content ledger holding the documents individually encrypted, and a transaction ledger holding the encryption keys on a series of ‘key rings’. The subject can give the certifier permission to put digitally certified documents on their key rings. The subject can give copies of the keys to inquisitors. A system can restrict the number or the timing of inquisitor examinations and records all inquisitions for the subject. This type of system meets such data protection standards as the ‘right to be forgotten’ and location of data storage. The subject ‘owns their own data’ and serves as the conduit, when needed, for communication between inquisitors and between certifiers, in full control. The ‘right to be forgotten’ is exercised by removing or losing a cryptographic key.

A simple example might be that you go to an identity certifier to encode your DNA, retinal scan, and photo, thus time-stamping your identity. Certifiers have no further access to the data. However, you can share the key to your identity chain with other people and organisation who will rely upon the fact that the data has been co-stamped by a trusted third party. Further developments in

[39] Z/Yen have developed similar systems, e.g. IDchainZ – www.idchainz.com

techniques such as homomorphic encryption and the use of zero-knowledge proofs may permit interrogation of MDLs while revealing the minimal amount of necessary data.

Simple and effective systems for KYC/AML/UBO are likely to be adopted by the financial services sector as they will make possible significant cost savings and enhance the customer experience. The establishment of an effective, widely accepted performance standard will greatly enhance market acceptance.

Effective Governance

Governance standards are essential for multi-organisational systems. The majority of respondents believed that MDLs used in commercial transactions will use privately permissioned access, which will not rely on proof-of-work, allowing permissioned individuals to write to private ledgers (aka proof-of-stake). Proof-of-work chains are essentially self-governing and self-correcting, with the chain supported by the majority of participants considered to be correct. With multi-organisation proof-of-stake MDLs, the persistence of data written to the ledger will require procedures for identifying who has permission to update the chain, how errors can be corrected, and how disputes between MDL participants regarding the veracity of a ledger can be resolved. The development of standards for trust structures is essential given the multi-party nature of MDLs (see Box 4.7).

Liability & Responsibility

In the future, as a new distributed ledger is created, an institution that supports it would not want to be a “deep pocket” target for a lawsuit from someone who claims its poor design caused damage. It is likely that institutions will insist that the MDLs they support will come with disclaimers and/or terms of use that severely limit liability[40]. A disclaimer is not a perfect shield from legal liability and will not protect an institution from liability if the institution knowingly engaged in fraud, though a well-crafted disclaimer can dramatically reduce the risk of liability. The development of a standardised approach to assessing the risks associated with liability arising from MDL data problems will assist in the development of disclaimers for multiparty agreements, and in the event of the failure of a MDL may indemnify participants from claims.

[40] Wright B 2016. *How to Cope with Block Chain Legal Liability* http://hack-igations.blogspot.co.uk/2014/10/open-ledger.html (retrieved 4 September 2016)

A good example of a system handling governance issues, as well as liability & responsibility for Public Key Infrastructure (PKI) certificates, among banks is IdenTrust (Box 4.7).

Box 4.7 Data Governance and Liability Standards Case Study - IdenTrust

IdenTrust was founded as a cooperative by a number of large international financial institutions, such as Citigroup and ABN AMRO, in April 1999. IdenTrust provides trusted identity solutions, recognized by global financial institutions, government agencies and corporations around the world, based on public key infrastructure (PKI).

The IdenTrust network enables organisations to manage the risks associated with identity authentication, working interoperably in countries around the world. Using the network minimises investment in creating new policies and legal frameworks, and deploys a range of products ensuring trust. The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (PLOT) to create a comprehensive environment for issuing trusted identities.

IdenTrust helps banks comply with the following regulatory requirements:

- AML - anti-money laundering
- FFIEC - Federal Financial Institutions Examination Council multifactor authentication banking guidelines
- HIPAA - Health Insurance Portability and Accountability Act
- KYC - Know Your Customer requirements
- SOX - Sarbanes-Oxley
- EU 8th Directive for tracking accountability

IdenTrust credentials provide three key capabilities:

Authentication	Proves Identity
Encryption	Safeguards content Ensures document integrity Eliminates pharming (man-in-the middle or DNS poisoning)
Digital Signing	Replaces 'wet' signatures Provides user-level signatures Enables straight-through processing (STP) (paperless workflows)

IndenTrust establishes a common and consistent set of rules for verifying someone or something’s identification, then translates that identity from a physical source into an electronic form, storing it in a portable form, with defined operational and technical elements. The ‘trust network’ has rules that govern how the digital identity will work, including what type of activities can be performed using the digital identity, and defines what will happen when something goes wrong, i.e. what are the legal implications, the forms of recourse, and the liability of the various parties.

Compliance

While it could be argued that compliance could be managed through the extension of an ISO 9000 quality management scheme, the cross-jurisdictional nature of MDLs may require the development of an addition to the ISO 9000 series. Equally, existing compliance standards, such as ISO 19600, BS 8453, or AS 3806 might well easily encompass MDLs.

Professional Standards

Standards are emerging for professionals, e.g. the CryptoCurrency Certification Consortium offers Certified Bitcoin Professional and Certified Bitcoin Expert qualifications. Several interviewees questioned the need for professional qualifications. Their argument was that MDLs are not particularly technically complex and traditional market means of assessing competence are sufficient.

Domain expertise was more nuanced. A number of interviewees expressed concern that some software developers had a limited understanding of the financial services eco-system. The view was expressed that, without an understanding of the framework of relationships and regulations facing financial services organisations, entrepreneurs operating in fintech would fail to comprehend potential systemic risks. This desire to have developers acquire domain expertise in order to practice their work competently is an old one and, while valid, is beyond the scope of this paper, e.g. health IT professionals, airline IT professionals, etc.

Sector Specific Standards for MDLs

The consensus among the individuals interviewed for this research is that the development of sector specific standards would enhance the attractiveness of MDL-based solutions. The need for the development of standards around identity, responsibility, liability and governance were raised by a large number of respondents.

5 Developing New Standards For MDLs

What Makes A Good Standard?

Review of the literature and discussion with stakeholders indicates that the following characteristics are the key features of a "world class" standard:

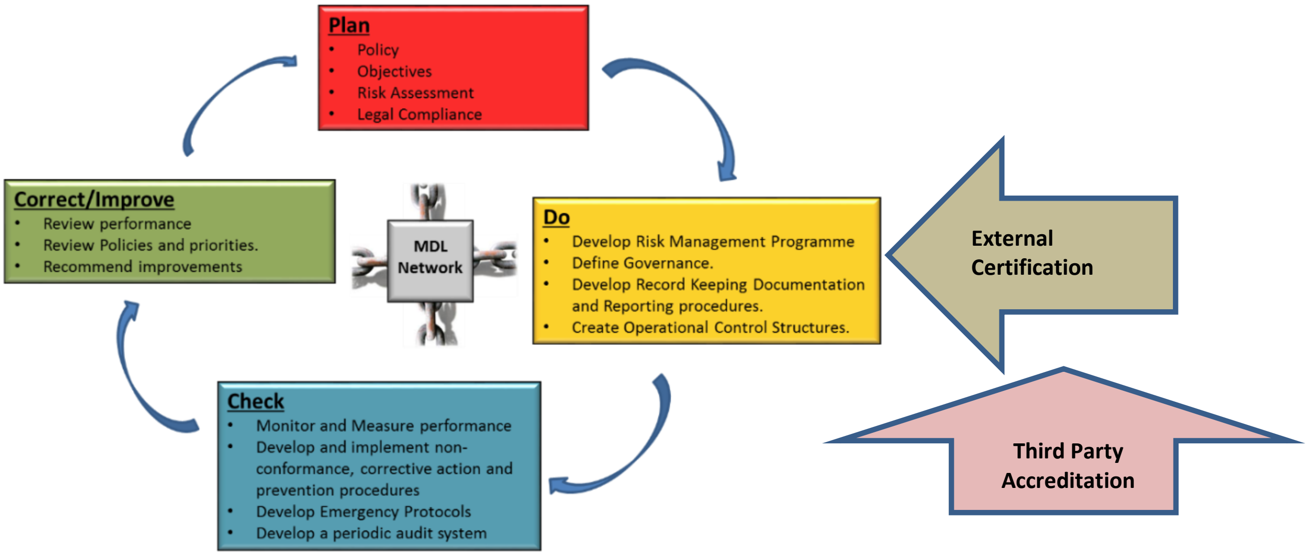
- ♦ **An open and transparent development process** where regulators pay attention to standard setting and competition because a standard constitutes a form of agreement between companies.[41] Competition rules usually do not allow companies to discuss and agree the technical developments of an industry among themselves. Discussions in the context of standard setting can, for example, provide an opportunity to reduce or eliminate competition, or in extreme cases lead to a "patent ambush". This is where a company involved in developing a standard hides the fact that it holds essential intellectual property rights over the standard being developed. It then starts asserting these intellectual property rights once the standard has been agreed and other companies are locked into using it;
- ♦ **Well defined objectives** that are expressed clearly and unambiguously. The standards setting body must ensure that these are reviewed on a regular basis in order to ensure that continues to meet the needs of clients;
- ♦ **Detailed Certification specifications** that clearly explain how conformity with the standard can be demonstrated;
- ♦ **Detailed Accreditation Specifications** clearly explaining the competencies certifiers have to demonstrate to prove they are qualified to issue certification.

Processes For Developing Standards

One of the strengths of voluntary standards is that they exist in a market and users are free to choose the most cost effective standard which meets their needs. Standards developers must balance the potential costs for standards users against the credibility of the standard. If the specifications, and thus burdens of implementation, are too high, users will seek lower specification standards. If the specifications are too low, users will see no advantage in seeking certification.

[41] Schellingerhout, R 2011. "Standard-setting from a competition law perspective" Competition Policy News Letter of the European Union No 1

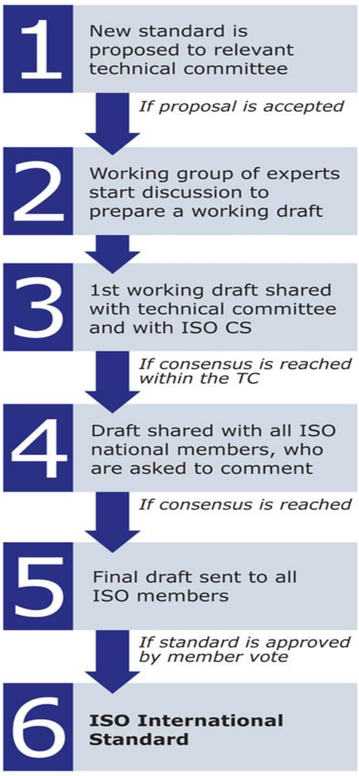
Figure 5.1 Process Flowchart For The Implementation Of A MDL Standard


Plan
• Policy
• Objectives
• Risk Assessment
• Legal Compliance
Correct/Improve
• Review performance
• Review Policies and priorities.
• Recommend improvements
MDL Network
Do
• Develop Risk Management Programme
• Define Governance.
• Develop Record Keeping Documentation and Reporting procedures.
• Create Operational Control Structures.
External Certification
Check
• Monitor and Measure performance
• Develop and implement non-conformance, corrective action and prevention procedures
• Develop Emergency Protocols
• Develop a periodic audit system
Third Party Accreditation

Standards developers must also ensure that there are effective and transparent certification and accreditation schemes in place to maintain confidence in the standard. There are three potential routes which can be used to develop sector specific standards for MDLs.

1 **The International Standards Organisation**. In order to pursue this route, it would be necessary to work with national standards institutions and wider stakeholders to propose a new standard to ISO/IEC JTC 1 the technical committee responsible for Information Technology. The process for development of an ISO standard is illustrated in Figure 5.2. The benefits of this process would include a clearly defined certification accreditation route and enhanced credibility for any standards created.

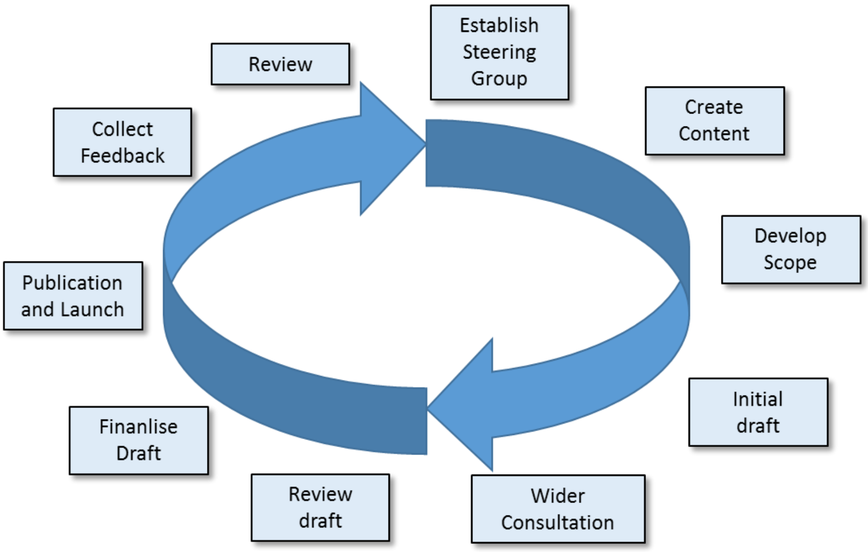
Figure 5.2 Process For Developing An ISO Standard


1
New standard is proposed to relevant technical committee
If proposal is accepted
2
Working group of experts start discussion to prepare a working draft
3
1st working draft shared with technical committee and with ISO CS
If consensus is reached within the TC
4
Draft shared with all ISO national members, who are asked to comment
If consensus is reached
5
Final draft sent to all ISO members
If standard is approved by member vote
6
ISO International Standard

Source: International Standards Organisation - How does ISO develop standards?

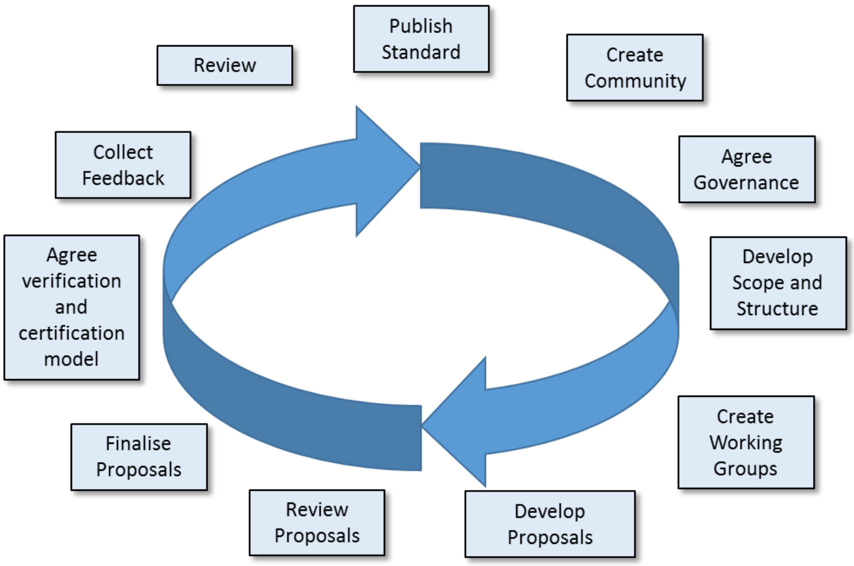
2 **National Standards Institutions.** The ANSI, BSI, DIN and other nationally based standards institutes have similar processes for the development of **Publically Available Specifications (PAS).** A PAS is a document that standardises elements of a product, service or process. PASs can be commissioned by individual companies, trade associations or government departments. The advantage of a PAS is that it is developed in consultation with relevant stakeholders and PAS specifications tend to be less onerous than full ISO standards. If a PAS proves popular it can be developed into an ISO standard.

Figure 5.3 Process For Developing A PAS



3 **Open process.** The development of a regulator-led open process, based on approaches similar to the Internet Engineering Task Force (IETF) Request for Comment (RFC) series, is an alternative route. While the development of open standards can be resource intensive, the advantage of this approach is that it is led by the practitioner community and can provide a robust product that this tailored to industry needs. However, for a standard produced in this manner to achieve credibility robust certification and accreditation systems must be developed.

Figure 5.4 Process For Developing An Open Standard



Professional Qualifications

While the unregulated nature of the Fintech sector is one source of its strength – innovation and competition run at an accelerated pace, resulting in new products and services that have the potential to transform the financial services sector - there is anecdotal evidence points to a lack of understanding of the fundamentals of financial services among some developers. One possible solution to this issue is the development of professional standards or extensions of existing ones, e.g. additional certificates and diplomas relating to MDLs in specific sectors. In the UK, the British Computer Society (The Chartered Institute for IT), already offers a charter scheme for its members. It may be possible to expand such a scheme to create a scheme for Chartered Financial Technologists.

One regulator stated that specific standards would have little impact impact upon innovation as: “In the majority of cases the burden of standards implementation would lie with the user rather than the developer”.

6. Findings

As the MDL community addresses the real and perceived risks associated with its technology, standards will emerge for people, processes, and products. The voluntary standards model offers a robust model, which has already gained some traction in the financial services sector (ISO Committee 68 for financial services has published over 50 international standards and has 21 more under development). Given the complex regulatory environment that commercial firms, especially financial services, operate in, ensuring MDLs fit within the existing standards framework is challenging, though iterative "standards for standards" such as PAS 99 or ISO 9000, may offer scope for expansion.

SWIFT concluded: "… full-scale standardisation of DLT/SC [distributed ledger technology/smart contract] use-cases is probably premature. However, even without a formal methodology, there is clear value today in re-using reference data standards and business content from messaging standards, most obviously ISO 20022 which has the widest industry coverage and an adaptable technical architecture. The benefits are twofold:

- ♦ Avoiding 're-inventing the wheel' in terms of business definitions;
- ♦ Facilitating interoperability amongst DLT implementations and with existing financial industry infrastructure including electronic messaging."[42]

We concur in a wider sense with SWIFT, including that:

- ♦ Existing regulations are, for the most part, sufficient to oversee the activities which are likely to benefit from MDLs.
- ♦ Technical operation standards are not necessary at this stage of the development of MDLs.
- ♦ Professional qualifications for developers and operators of MDLs are not yet needed.
- ♦ There may be scope to develop a carbon standard for cryptocurrencies.
- ♦ Sector specific standards are desirable and would benefit:
  - ➢ developers, through enhanced trust and understanding of the technology by users;
  - ➢ users, through the creation of a trust framework that manages risk;
  - ➢ regulators, by limiting threats to the integrity and reputation of markets.
- ♦ Standards would be particularly beneficial in the areas of:
  - ➢ taxonomies & performance;

[42] "Distributed Ledgers, Smart Contracts, Business Standards and ISO 20022", SWIFT Information Paper (September 2016) - https://www.swift.com/node/39911

  - ➢ data governance & liability ;
  - ➢ commercial governance & liability standards.
- ♦ There are a number of routes that can be taken to develop sector specific standards; however, all of them depend on the establishment or use of a robust verification and certification process.

In conclusion, the establishment of a voluntary standards market or markets may be beneficial in promoting the take up of MDLs by providing certainty to both users and developers, while assisting regulators in fulfilling their duties. A PAS route seems the most likely, probably three separate PAS's for 'taxonomies and performance', 'data governance & liability', and 'commercial governance & liability'. Further consideration is needed about the scope of 'taxonomies and performance', 'data governance & liability', and 'commercial governance & liability' standards. And of course, who is prepared to lead and what group is prepared to pay to take these forward?

Acknowledgements

We thank all those who have contributed time and expertise to this research. Any misinterpretations or errors are, of course, our responsibility. Contributions were for the most part given personally, and do not represent the views of any organisation. John Bullard was a particular help in understanding ‘trust networks’, and Colin Southall on the DAO. Professor Mike Smith and Bernard Manson of Z/Yen were of particular help in supplying technical background. We would like to thank the many people working at the following organisations for helping us, without in any way implying that they or their organisations endorse our findings.

ACORD
Alcova Asset Management
Alderney Electronic Gaming Commission
Ásta Guðrún Helgadóttir MP, Iceland
Bank of England
Barclays
BigchainDB
Blockchain.info
BNY Mellon
Bolero
BSI
Cambridge Blockchain
Capital Law
Cardano Foundation
Commonwealth Partnership for Technology Management
Coinsilium
Consensys
COOConnect
Credits
Cruxy & Co
CryptoCurrency Security Standard
Cynation
DasCoin
Deutsche Bank
Deutsche Börse
Digital Catapult
Digital Strategy Associates
Distlytics
DLA Piper
DTTC
Dun and Bradstreet
ElectriChain
Ethereum Foundation
Financial Conduct Authority
Financial Stability Board
Finceler8
Fintech Circle Innovate
Consensys
Freshfields Bruckhaus Deringer LLP
Harrington Star
Harvard Law School
Hill Hofstetter
ICAP
IHS Markit
Illuminate Financial
Innovate Finance
International Association of Insurance Supervisors
International Securities Association for Institutional Trade Communication
Kingston Smith
King & Wood Mallesons
Kynetix

Liberty Re
Linear Investments Ltd
Lite Hide
Lloyd’s of London
London Market Group
Lykke
Moscow Stock Exchange
Norton Rose Fulbright
National Standards Authority of Ireland
Object Chain
Options IT
PwC
R3
SAP
SCOR
Scotiabank
Société Générale
Solar Coin
States of Alderney
SWIFT
Technology in Business
Trading Screen
Tradle
Trunomi
UBS
United Kingdom Accreditation Service
United Kingdom Department for Business, Energy & Industrial Strategy
United Kingdom Digital Currency Association
University College London
Vestra Wealth Management

APPENDIX A – Sample Existing Standards Applicable To MDLs

Area	**MDLs (general)**	**Finance and Insurance**	**Internet-of-things**
Technical	♦ SQL (ANSI, ISO) ♦ XML ♦ ISO/IEC 20800 series metadata standards ♦ RFC 3161 time-stamping ♦ Secure Hash Standards - Algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256	♦ ACORD Standards for Insurance Documentation ♦ SWIFT Information Transmission Standards ♦ ISO 20022 Financial industry messages ♦ MDDL The (Financial) Market Data Definition Language ♦ InterLedger Protocol (Ripple) ♦ Chain Open Standard (Chain OS1) ♦ CryptoCurrency Security Standard (CCSS) ♦ Payment Card Industry Data Security Standard	♦ ADEPT ♦ New – ISO TC/307 Project – "Scope: Standardisation of blockchains and distributed ledger technologies to support interoperability and data interchange among users, applications and systems."
Governance & Process	♦ ISO/IEC 20000 IT Service management ♦ COBIT 5 Framework for IT management ♦ BS11000 Collaborative Business Relationships	♦ BS 8453 Compliance Framework for Financial Services ♦ ISO 31000 Risk Management Standard ♦ ISO 9001 Quality Management ♦ SAS 70 Auditing of	♦ ISO 31000 – Risk Management Standard ♦ ISO 9001 – Quality Management ♦ ISO 14000 – Environmental Management ♦ ISO 27000 – Information

	♦ CrytpoCurrency Certification Consortium (C4)	Financial Controls ♦ ISO 22301 Business Continuity ♦ NFPA 1600 ♦ CIIA Internal Audit Code ♦ G20/OECD Principles of Corporate Governance 2015 ♦ ISO 10002 complaints	Security Management ♦ ISO 19600 – Compliance Management Systems
Legal	♦ New York State Department of Financial Services “Bit-License”	♦ FATF Recommendations on AML & KYC ♦ EJML Steering Group Guidance on AML & KYC ♦ CAMS anti-money laundering specialisation ♦ MIFD Markets in Financial Services Directive ♦ Bitcoin Swap Standards (Tera Group with CFTC) ♦ Health Insurance Portability & Accountability Act	♦ CE mark ♦ 2010/30/EU Energy Labelling Framework Directive ♦ OHSAS 18001 ANSI/AIHA Z10-2005, CSA Z1000-06, UNIE 81900, AS/NZS 4801:2001 Occupational Health and Safety Standards ♦ IEC 61508:2001 Functional safety of electrical/ electronic/ programmable electronic safety-related systems

APPENDIX B – Case Studies Of Cryptocurrency Governance Issues

The DAO

The DAO (Decentralized Autonomous Organization) was launched on the Ethereum blockchain on 30 April 2016 with a website and a 28-day crowdsale to fund the organisation. By 21 May it had raised capital of more than US$150 million from more than 11,000 investors. On 17 June an unknown attacker ’stole’ around 3.6M ‘ether’, Ethereum’s online currency similar to Bitcoin, from The DAO. At the time the currency valuation of 3.6M ether was about $55 million dollars and represented around a third of The DAO’s assets.

The DAO was intended to operate as a hub that dispersed funds in ether to suitable projects. Investors received voting rights by means of a digital share token and voted on proposals that were submitted by ‘contractors’ while a group of volunteers called ‘curators’ checked the identity of people submitting proposals and made sure the projects were legal before ‘whitelisting’ them. The profits from the investments would then back to its stakeholders.

The underlying technology powering The DAO was a ‘blockchain’, similar to Bitcoin, overlaid with ‘smart contracts’. The DAO was controlled by the votes of its members (anyone who transferred ether to it) and transactions occurred automatically once enough members voted for them. A vulnerability in the code was exploited by the attacker, who used a Race-To-Empty or Recursive Call attack, to appropriate ether.

The immediate loss to DAO investors was compounded by a loss of confidence in Ethereum as a whole. Complex legal questions remain over whether the attack was really ‘theft’. In effect, the Ethereum project claimed to “let the code” decide, and the code decided to transfer 3.6M ether to an account. However, the eventual solution, a ‘hard fork’ that moved the ‘stolen’ Ether back into a new version of the DAO, in effect replaced ‘tyranny of the code’ with ‘tyranny of the majority’.

Fundamentally, the DAO attack raises serious questions about the types of safeguards that investors should have with such collective investments and the governance issues of the wider system for making such decisions.

Sources:
http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/

http://www.forbes.com/sites/jonathanchester/2016/06/21/can-the-50m-heist-of-the-dao-take-down-bitcoins-rival-blockchain/#da2eb9c7bcef
http://www.financemagnates.com/cryptocurrency/bloggers/the-effects-of-the-dao-and-bitfinex-hacks-on-bitcoin-exchanges/
https://cointelegraph.com/news/what-we-learned-about-technocratic-fallacies-from-dao-collapse (Retrieved 20 August 2016)

Mt. Gox

Mt. Gox was a Bitcoin exchange based in Tokyo, Japan. It was launched in July 2010, and by 2013 was handling 70% of all Bitcoin transactions In February 2014, the Mt. Gox company suspended trading, closed its website and exchange service, and for bankruptcy. In April 2014 the company began liquidation proceedings and announced that around 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time.

Subsequent investigations by the Tokyo police have led to the arrest of the former CEO, who has been charged with fraud and embezzlement. However, investigative journalists have suggested that the spectacular collapse of the company may have been the result of a perfect storm of a series of hacking attacks, the unprecedented rise in the value of bitcoin (from $13 at the start of 2013 to more than $1,200 at its peak), poor financial practices within the company, and the seizure of assets by US regulators.

On 15 May 2013 the US Department of Homeland Security (DHS) issued a warrant to seize money from Mt. Gox's US subsidiary’s account with payment processor Dwolla (an e-commerce company that provides an online payment system and mobile payments network). US Immigration and Customs Enforcement claim that the subsidiary, which was not licensed by the US Financial Crimes Enforcement Network (FinCEN), was operating as an unregistered money transmitter in the US.

Mt. Gox’s origins as a platform for exchanging fantasy game cards (Mt. Gox is an acronym of Magic: The Gathering Online Exchange) and the backgrounds of its CEO and board meant it was ill suited to manage the sudden rise in value of the commodity it traded. Poor security which made it a target for hacking and the failure of the board to keep track of the regulatory environment, particularly with respect to anti-money laundering regulation, are salutary lessons. Mt. Gox gave up its plan to rebuild under bankruptcy protection on 16 April 2014, and asking a Tokyo court to allow it to be liquidated.

Sources:
http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html
http://www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange/
http://www.wired.com/2014/03/bitcoin-exchange/
https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency (Retrieved 21 August 2016)

Bitfinex

On 2 August 2016, Hong Kong-based Bitcoin exchange Bitfinex, one of the largest Bitcoin exchanges, announced that hackers had stolen 119,756 bitcoins from clients' accounts, approximately US$65M at the time. The source of the vulnerability appears to have lain in how Bitfinex structured its accounts. Some commentators speculated that pressure from the US Commodity Futures Trading Commission (CFTC) over alleged trading violations led to Bitfinex eschewing the use of ‘cold storage’ for multi-signature wallets (where keys are divided among a number of owners to manage risk).

The immediate aftermath of the theft saw a 20% drop in the value of bitcoin. A subsequent announcement by Bitfinex that all its customers (regardless of whether they had suffered a loss) were likely to receive a 30% ‘haircut’ on their funds sparked a race for litigation. As of late 2016, Bitfinex is still trading and claiming it will recompense customers.

Sources:
http://www.coindesk.com/bitfinex-warns-customers-to-halt-deposits-after-suspected-hack/
http://www.coindesk.com/bitcoin-price-slumps-following-bitfinex-outage/
https://www.cryptocoinsnews.com/breaking-bitcoin-exchange-bitfinex-hot-wallet-hacked/
http://www.jdsupra.com/legalnews/the-aftermath-of-the-bitfinex-hack-38645/
(Retrieved 21 August 2016)

APPENDIX C – Technical Background On MDLs

MDL Technology

The key purpose of MDL technology is to produce a data file which is guaranteed tamper proof, and can be shared between users. All users can read the file and check its consistency, and one or more users will be able to update the file. A configuration enabling update by multiple users can remove the need for a central owner.

The basic tool is a 'hash' embedded in the data file to guarantee that the data has not been tampered with. The hash is produced by an arithmetic function taking as input every bit (0 or 1) of the data and changing its output unrecognisably if a single bit is changed or added.

Thus, for example, SHA-256, a commonly used hash function, gives the following output for data "abcdefghijklm" and "abcdefghijklo" – two strings differing only in the last letter and there only by a single bit in the computer code:

"ff10304f1af23606ede1e2d8abcdc94c229047a61458d809d8bbd53ede1f6598"
and
"880433bd8ba16631775ddfba51d505df76d8a3420db9e21d123c2fcbd46fe48f"

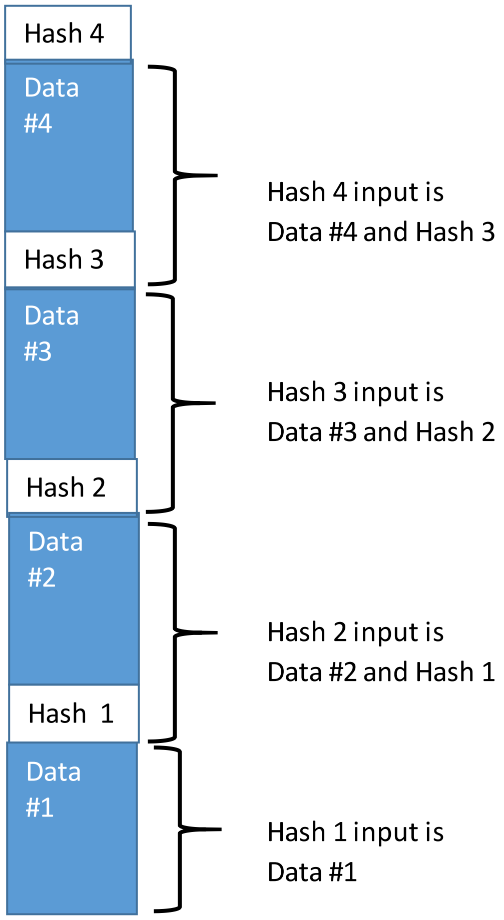
Each output is a number which would be about 77 digits in decimal and is represented here slightly more efficiently in base 16 – hexadecimal – where the numbers from 10 to 15 in decimal are represented as 'digits' a, b, c, d, e, f.

Given a SHA-256 code for a random file, your chance of finding a second file with the same code – assuming you have a computer per person on the planet each capable of processing a billion billion billion files per second, and the time available since the big bang – is infinitesimal: about one in a million billion billion billion.

In a MDL, a hash is appended after each new block of data. This takes as input not only all of the new data but also the previous hash. This guarantees that any change of data anywhere in the entire file will create an inconsistency in the final hash.

The integrity of the process is underwritten by distributing copies of the MDL file or changes to the file to all users each time there is an addition of a data block and hash. Everyone thus has an updated copy of the file and can check the consistency of the hashing. This also allows for different users (with appropriate permission) to update the file, subject to there being rules in place to deal with simultaneous updates. A MDL file therefore looks like:

Blockchain Structure


Hash 4
Data #4
Hash 3
Data #3
Hash 2
Data #2
Hash 1
Data #1
Hash 4 input is Data #4 and Hash 3
Hash 3 input is Data #3 and Hash 2
Hash 2 input is Data #2 and Hash 1
Hash 1 input is Data #1

By removing the hashes, you recover a normal data file which can contain any set of data you wish. This could include databases, word documents, PDFs, spreadsheets, and photographs or video or audio files. The MDL can thus be used to replace any paper or electronic files and to transmit the whole with perfect integrity and version control each new version will require a new hash).

An alternative structure is to include just the hashes in the distributed MDL and to store the data elsewhere. This means that the MDL itself is much shorter and there is potentially better data protection, while the core capability of providing proof that the data blocks were added at specific times is maintained. However, there now has to be a separate process for maintaining distributed copies of the data blocks, raising new issues of governance, process, and risk.

Given that MDL guarantees accuracy of data, it can be used for **Smart Contracts.** These are contracts embedded as code in the MDL and executed automatically when some trusted external data source hits a defined value. An example with relevance to insurance might be a weather insurance contract which pays out if the rainfall in a specific location in a specific month exceeds 7cm, as defined by a data output from the UK Met Office.

MDL Update Process

The internal design of the MDL is described above, but there also needs to be a process by which the MDL is extended each time there is a new block of data to be added. This mechanism for update must ensure the following:

- data added to the MDL maintains the integrity of the MDL structure;
- update is timely and new data is broadcast quickly to all users of the MDL;
- the process is resilient against individual users being unable to access the system;
- where there is an update of the same MDL by different nodes with different data, resulting in two incompatible versions of the MDL broadcast (a 'fork'), there is a process to ensure that the situation is resolved quickly and the integrity of the MDL data is maintained.

There are different technical and governance models for achieving consensus for a permissioned MDL. The choice of mechanism will depend on factors such as the application being supported and the number of active users. In a regulated environment, there may be a need for a 'user of last resort' which maintains a current copy of the MDL and contracts to rebroadcast if required.

Part of the process of implementing any MDL application will be to optimise the governance and technical framework for the update mechanism. There are many technical solutions for validating new transactions and adding a new block of data to the MDL.

Perhaps most simply, high-volume ledger recording, such as data logging, may allow a stream of transactions to be added to a MDL by any user. If there is little chance of fraud, then the mere act of adding the data, timestamped if required, may be a sufficient level of validity. The user adding a new block of data will generally include a block of cryptographic information to prove their own identity and provide evidence it has carried out some validation.

A permissioned MDL can establish a more sophisticated update process based on a voting system. At its simplest, a single central party could have the right to validate and update the MDL – a single voter. Given the reason for choosing MDL technology in the first place, it is more likely that governance would require some sort of involvement by all participants. This might require unanimity, or it might require a threshold number of participants. Many other models are possible.

Any 'democratisation of data' raises issues of governance, risk, and cost, but working solutions exist for these within existing applications.

Cryptocurrencies

Another definition of cryptocurrency, this time from 'CryptoCoin News', is "a medium of exchange like normal currencies such as USD, but designed for the purpose of exchanging digital information through a process made possible by certain principles of cryptography."

Cryptocurrency applications such as Bitcoin are built on MDLs, but they add significant amounts of validation technology. The distinguishing computer function of a cryptocurrency is how it validates new transactions and avoids people cheating by writing invalid transactions. The intense interest among technologists in Bitcoin derives from its innovative approach to achieving distributed consensus on new transactions: the 'mining' process.

Bitcoin's mining uses a 'proof-of-work' test to assign who can update the MDL. On each iteration of the MDL, this asks users to find – by running a hashing function on random numbers – a number which gives a SHA-256 hash within a target range. The more computing power a user puts in, the more likely it is to be first to the solution and hence to have the right to update the MDL – and to receive a prize of newly minted Bitcoins which is the economic drive for participation in the process. Many other cryptocurrency systems, such as Ethereum, use a similar approach.

Bitcoin's mining carries a heavy overhead in terms of cost and speed. The process is energy-intensive meaning that the cost of writing a Bitcoin transaction is rather high (tens of cents or dollars) and is likely to remain high. The mining process is also slow, on the order of about ten minutes to process a new block of data. This is a dynamic environment and Bitcoin may get cheaper and faster, but at the moment it can process only about seven transactions per second at peak volume.

A suggested alternative approach is ‘proof-of-stake’ which requires users to prove ownership of a certain amount of currency or to use some of their ‘stake’ in the currency to indemnify transactions against fraud in order to take part in the next update of the MDL. The most significant proof-of-stake environment is Ripple. The debate on whether ‘proof-of-stake’ is a viable approach is heated, and is outside the scope of this paper. To date, proof-of-stake approaches have been overshadowed by proof-of-work for unpermissioned MDLs.

The Long Finance initiative grew out of the London Accord, a 2005 agreement among investment researchers to share environmental, social, and governance research with policy-makers and the public. In 2007 Long Finance was established more formally by Z/Yen Group and Gresham College with support from the City of London Corporation with the aim of exploring long-term thinking across a global network of people.

"When would we know our financial system is working?" is the question underlying Long Finance's goal to improve society's understanding and use of finance over the long term. In contrast to the short-termism that characterises today's economic views the Long Finance time-frame is roughly 100 years. Long Finance aims to:

♦ expand frontiers - developing methodologies to solve financial system problems;
♦ change systems - provide evidence-based examples of how financing methods work and don't work;
♦ deliver services - including conferences and training using collaborative tools;
♦ build communities - through meeting, networking and events.

Long Finance runs programmes exploring four major themes:

♦ **London Accord** – looking at environmental, social, and governance investment research issues;
♦ **Financial Centre Futures** – seeking to explore how finance might work in the future;
♦ **Meta-Commerce** – aiming to identify and structure the critical questions underlying the long-term viability of the financial system;
♦ **Eternal Coin** – encouraging a global discussion on the nature of money and the concept of value.

www.longfinance.net

A report prepared by Z/Yen Group
Principal authors: Professor Michael Mainelli & Simon Mills

Z/Yen Group Limited
41 Lothbury, London EC2R 7HG, United Kingdom
+44 (20) 7562-9562 (telephone)
hub@zyen.com (email)
www.zyen.com

SPONSORED BY

STATES OF ALDERNEY

The States of Alderney is the legislative assembly of the Channel Island of Alderney, which remains a separate jurisdiction within the Bailiwick of Guernsey. The main economic drivers on Alderney include business services, finance, eGaming, tourism, and energy. Alderney seeks to become the leading centre for regulation and standards for mutual distributed ledgers.
www.alderney.gov.gg

pwc

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.
www.pwc.com

CARDANO FOUNDATION

Cardano Foundation is a blockchain and cryptocurrency organisation based in Zug, Switzerland. The Cardano Foundation is dedicated to act as an objective, supervisory and educational body for the Cardano Protocol and its associated ecosystem. The Foundation aims to influence and progress the emerging commercial & legislative landscape for blockchain technology and cryptocurrencies. Its strategy is to pro-actively approach government and regulatory bodies and to form strategic partnerships with businesses, enterprises and other open-source projects. The Foundation's core mission is to "standardise, protect and promote" the Cardano Protocol technology.
www.cardanofoundation.org