

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers (aka Blockchain)





RESPONSIBILITY WITHOUT POWER?
THE GOVERNANCE OF MUTUAL DISTRIBUTED LEDGERS
(AKA BLOCKCHAIN)

Simon Mills & Bob McDowall

JULY 2017



Z/Yen Group Limited
41 Lothbury, London EC2R 7HG, United Kingdom
+44 (0) 20 7562-9562 (telephone)
hub@zyen.com (email)
www.zyen.com

© Z/Yen Group Limited, 2017

Foreword

Much has been written about the power and scope of Mutual Distributed Ledger (MDL, aka Blockchain) Systems. One of the Cardano Foundation's main objectives is to help shape the governance landscape surrounding emerging distributed technology. We believe that it is vital that the practice of good governance is incorporated into MDL systems, if they are to establish credibility and gain widespread acceptance.

Amidst the rush to find new applications for this versatile technology, this report provides an overview of the challenge of governing MDL networks. Its aim is to identify the critical components of effective governance in order to provide a roadmap for developers and users alike.

Michael Parsons FCA, Chairman of the Cardano Foundation

Contents

Executive Summary	4
Background And Methodology	8
Part 1 The Fundamentals Of Governance	9
1.1 Introduction	9
1.2 The Governance Of MDLs - Does ‘One Size Fit All’?	11
1.3 What Are The Governance Challenges Facing MDLs?	14
1.4 How Should MDL Governance Structures Be Organised?	15
1.5 The Architecture Of Governance	18
1.6 The Role Of Trust In Trustless Systems	20
1.7 Ethics And Social Norms	21
1.8 Market Structures And MDLs	22
Part 2 Governance Structures For MDLs	25
2.1 Introduction	25
2.2 Governance Structures For Public MDLs	25
2.3 Governance For State-Sponsored MDLs	28
2.4 Governance For Private And Consortium MDLs	32
2.5 Project Governance For MDLs	33
2.6 Does The Governance Of Legacy IT Systems Hold Lessons For MDLs?	34
Part 3 Tools And Techniques For The Governance Of MDLs	36
3.1 The Foundations Of Good Governance	36
3.2 Tools For Effective Governance	37
CONCLUSION	42
Glossary	45

Executive Summary

Effective governance in Mutual Distributed Ledgers (MDL) systems relies on people rather than software and should seek to answer four critical questions:

- ◆ How are rules created for the ledger and who oversees their application?
- ◆ What happens in the case of dispute?
- ◆ Who is allowed to change the software application and the data?
- ◆ How are security, risk and performance managed and reported?

The Fundamentals of Governance for MDLs

The primary goal of governance in MDL networks is to enhance trust. Although MDLs are often referred to as 'trustless networks' due to the way that transactions are managed, in reality, trust is a critical factor in the success of an MDL. Instead of trusting laws and institutions, users are expected to trust stakeholders, programmers and those who are technically accomplished enough to verify the code. Ensuring users and providers of MDL services agree on terms of service and acceptable use is a prerequisite for governance. An MDL without governance is unlikely to achieve its long-term business goals as it will lack a coherent strategy or the means to implement it. It will also be unable to respond effectively to threats as it will lack effective risk management procedures.

Governance, which enhances trust in MDL systems, rests on three pillars:

1. **Architecture:** The role of the governance structure, its composition, remit, powers, responsibilities, and relationship with users is a critical component.
2. **Accountability:** Effective governance of MDLs creates confidence for stakeholders. Appropriate confidence is enhanced when a governance structure is accountable to its stakeholders, transparent and predictable in its decision-making, and has strong ethical foundations, particularly with respect to access to justice.
3. **Action:** The governance structure must develop strategic and risk management plans, which are delivered through effective performance management frameworks. Confidence can be enhanced through the use of voluntary standards to verify independently performance metrics and systems created to compile them.

The Architecture Of Governance

There are two type of ledger:

- ◆ un-permissioned ledgers where users are anonymous and there is no need to register with a central authority and;
- ◆ permissioned ledgers, which require the identity of users to be whitelisted or black-listed through some type of Know Your Customer (KYC) procedure.

Responsibility Without Power?
The Governance Of Mutual Distributed Ledgers

These two types of ledger lend themselves to four different use classes, each of which requires different governance structures. Table 1 illustrates the four different use classes and the types of governance structures they require:

Table 1 MDL Use Classes And Their Corresponding Governance Structures

Type of MDL	Use Class	Governance Structure
Un-permissioned	Public MDLs: Little formal governance structure. <i>E.g. Crypto-currencies</i>	Co-operative: An autonomous association, jointly owned and democratically controlled.
Permissioned	State sponsored MDLs: Governance structures of sponsoring agencies grafted on. <i>E.g. land registries or identity</i>	Appointed Board: Board members are appointed by stakeholders, or the board itself, to bring particular knowledge and skills to the table.
Permissioned	Private MDLs: Highly defined governance structure. <i>E.g. platforms for blockchain-based applications for business ecosystems.</i>	Oligarchy: The individuals that comprise the board are the owners or stakeholders.
Permissioned	Consortium MDLs: Established and managed by a group of organisations rather than a single entity, likely to have a complex governance structure. <i>E.g. Financial Services or Internet of Things (IoT) platforms.</i>	Membership: Board members are elected to their positions and tenure is for a fixed period.
Permissioned	State-Sponsored and Consortium MDLs (see above)	Representative: For organisations that wish to have members who are enterprises instead of individuals. This structure may be appropriate for both consortium and state-sponsored MDLs.

Accountable Governance Structures

Governance operates at three levels in organisations. Market governance addresses the system of laws and social norms within which entities operate. Corporate governance addresses the system of rules, practices, and processes by which goals are set. Project governance addresses the processes and procedures for the control of projects and programmes.

- ◆ Market governance is external to the organisation. It plays a critical role in enhancing trust in MDL networks, including consideration of ethics and ethical behaviour of the service provider and its users. Of particular importance is the consideration of users' access to 'judicial' services. Effective systems to handle violations of the transaction process, such as breach of confidentiality or identity fraud, are essential if MDL technology is to play a significant role in commercial transactions.
- ◆ Accountability to stakeholders is critical for corporate governance and has direct relevance to MDLs, as accountability enhances the confidence of users in governance structures. Accountability confers legitimacy on decision making and can be demonstrated by establishing and disclosing the respective roles and responsibilities of the board through creation of appropriate decision making structures and establishment of formal and rigorous reporting processes.
- ◆ MDLs potentially carry a high strategic impact for individuals, organisations, and networks. Effective project governance will enable organisations to manage the impact of adoption of MDLs.

The Governance of Action In MDL Systems

The most appropriate method for the governance of software development is a subject of debate. Once an MDL network is established, the tools for the effective governance of MDLs are broadly similar to the tools for effective governance of any entity. Strategic plans set priorities, focus energy and resources, and strengthen operations. Strategic plans ensure that stakeholders are working toward common goals that establish agreement around intended outcomes. Stakeholders must assess and adjust the network's direction in response to a changing environment.

Performance management frameworks identify performance benchmarks and monitor progress against the goals contained in the strategy. The frameworks ensure that performance improves over time. Performance management standards have yet to be developed for MDLs, although a range of standardised business tools, such as COBIT 5, which is currently used in project and IT management, are applicable to MDL networks.

Risk management plans should analyse the likelihood of adverse events and their likely impact on the MDL and its users. Strategies should be developed to mitigate and manage these risks. Significant risks include changes in the business or regulatory environment, which impact the MDL and the stakeholders.

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

Auditing and reporting arrangements should enforce accountability and promote trust in governance arrangements. Robust auditing and reporting systems are particularly important for MDL systems used within the financial services sector, where sanctions and penalties for violation will result from breaches of regulations. Confidence in reporting arrangements can be enhanced through the use of third party audits or conformity assessments

MDLs should be designed to facilitate audit. Although MDLs are designed to promote disintermediation, central third parties will still be needed to:

- ◆ Confirm the existence of the asset to be traded, be it money, securities, or other assets.
- ◆ Verify identity.
- ◆ Provide oversight and reassurance on Know Your Customer (KYC) and Anti Money-Laundering (AML).
- ◆ Ensure compliance with law and regulators.
- ◆ Guarantee the rights of those participating in the transaction.

Key Issues For The Governance Of MDLs

Ambitious claims have been made about the ability of MDLs to deliver financial services without financial intermediaries, transaction platforms without the need for third parties, and national archives with reduced administrative costs.

The systems that MDLs seek to supplant have evolved over decades to provide high levels of security, reliability, and predictability. In order to reach their full potential adoption, MDLs must ensure that users have confidence in their ability to offer similar assurances. Effective governance is key to providing this assurance.

Table 6 (page 42) contains a checklist of appropriate considerations for the governance of MDL networks.

Background And Methodology

The Cardano Foundation commissioned this study in April 2017 in order to examine the issues associated with the governance of mutual distributed ledgers (MDLs, aka blockchain).

Methodology

This research paper was developed through desktop research, supplemented by discussions with practitioners and stakeholders, as well as a conference and a webinar.

The focus of the discussions sought to identify stakeholder views on:

1. The governance challenges associated with the uptake of MDLs across a range of sectors.
2. Current approaches and thinking.
3. The ways that these challenges may be addressed by developers and users.

Interviews were conducted on a semi-structured basis and combined a pre-determined set of open questions with the opportunity to explore particular themes or responses further. Participants were interviewed either in person or by telephone and were selected to represent the following groups of stakeholders:

- ◆ Software developers and suppliers of blockchain services
- ◆ Regulators
- ◆ Legal professionals
- ◆ Accounting professionals
- ◆ Financial services professionals
- ◆ Academics

This study seeks to be rapid and relevant. No attempt has been made to estimate the potential costs of governance failures to users or markets. Such a high-level process does not guarantee 'accuracy', but we believe that it provides a roadmap for organisations seeking to find a solution to this urgent issue. The challenge of the interoperability of MDL networks with existing legacy systems is beyond the scope of this report.

Part 1 The Fundamentals Of Governance

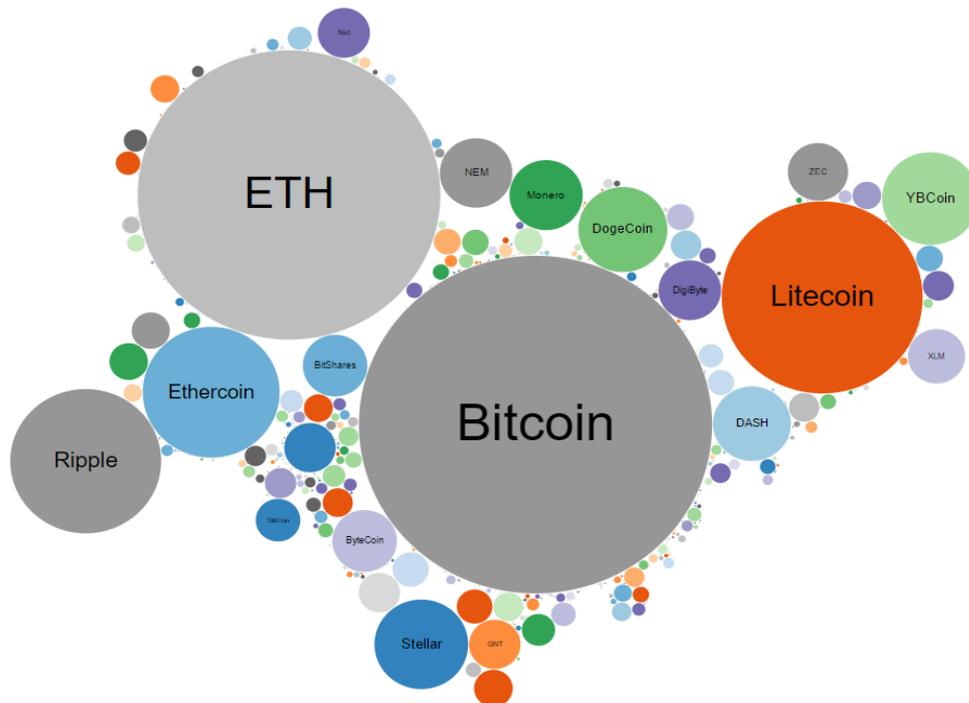
1.1 Introduction

Mutual Distributed Ledgers (MDLs, aka blockchain) are systems that enable parties who don't fully trust each other to form and maintain consensus about the existence, status, and evolution of a set of shared facts.¹

The core MDL technology has been available for some time, but MDLs rose to prominence following the publication of Satoshi Nakamoto's seminal paper "*Bitcoin: A Peer-to-Peer Electronic Cash System*" in 2009,² which combined hashing techniques and writing and distributing data to a chain of blocks, in order to develop a non-fiat "crypto-currency".

Following the launch of bitcoin in 2009, a large number of other crypto-currencies have been developed (over 4000 at the time of going to press³ - see figure 1). This explosion of interest spurred developers to seek other uses for distributed ledgers.

Figure 1 Total Exchange Trading Volumes For Crypto-currencies Over A 24 Hour Period in 2017



Source: Eisenberg C 2017⁴

¹ Brown R 2016 "On distributed databases and distributed ledgers" <https://gandal.me/2016/11/08/on-distributed-databases-and-distributed-ledgers/>

² Nakamoto, S 2009 "*Bitcoin: A Peer-to-Peer Electronic Cash System*" <https://bitcoin.org/bitcoin.pdf>

³ Eisenberg C 2017 "Crypto Coins List" <https://www.cryptocoincharts.info/coins/info>

⁴ Eisenberg C 2017 "Graphical Crypto Currency Comparison" <https://www.cryptocoincharts.info/coins/graphicalComparison>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

Although the rise of crypto-currencies has overshadowed their supporting technology, realisation has grown, particularly in the financial services sector, that MDLs have a much broader base of potential uses.

Box 1 *MDLs Defined*

A mutual distributed ledger is a computer data structure with the following defining attributes:

- ◆ Mutual – shared across organisations, owned equally by all, and dominated by no-one.
- ◆ Distributed – copies of the data are spread across multiple locations. Users can keep their own copy, thus providing resilience and robustness.
- ◆ Ledger – the structure is immutable. Once a transaction is written it cannot be erased and, along with multiple copies, this means that the ledger’s integrity can easily be proven.

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

MDLs securely store transaction records in multiple locations with no central ownership. MDLs allow groups of people to validate, record, and track transactions across a network of decentralised computer systems.

They are suitable for a range of applications including;

1. **Transactions** – particularly for payments, transfers, and insurance and financial services administrative processes. The Bank of England’s (BoE) fintech accelerator has recently teamed with Ripple for a cross-border payments proof of concept. In the Middle East, the National Bank of Abu Dhabi has become the first bank in the region⁵ to introduce real-time cross-border payments on Ripple’s blockchain network.
2. **Records** – such as registries, time stamping, and data logging. Sweden’s land registry authority (Lantmäteriet) began testing a way to record property transactions on a blockchain in June 2016⁶.

⁵ Andreasyan T 2017 “*BBVA and Ripple complete blockchain cross-border money transfer pilot*”
<http://www.bankingtech.com/806262/bbva-and-ripple-complete-blockchain-cross-border-money-transfer-pilot/>

⁶ Wong J 2017 “*Sweden’s blockchain-powered land registry is inching towards reality*”
<https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

3. **Identity** – including Anti Money Laundering (AML), Know Your Customer (KYC) and state records (Estonia has successfully pioneered a universal, national identity scheme using a type of MDL)⁷.
4. **Internet-of-Things** (IoT) – using the Internet to connect computing devices embedded in everyday objects, enabling them to send and receive data. Developing ledgers detailing the permissions associated with this data transfer, as well as logging and storing the data itself is a technical challenge for which MDLs are well suited. A number of corporations are developing platforms to enable secure IoT systems, including IBM, which is developing the MDL based Watson IoT platform.⁸

When an MDL platform is developed, organisations must establish an agreement that governs the fundamental rules of the new network. This can be a daunting process, as organisations have differing policies and protocols for the administration of their operations.

An organisation considering joining an existing MDL network has to evaluate the benefits of the new arrangement against the potential risks of ceding control of data, processes, and systems. Trust in the system is required. Trust extends beyond the effectiveness of the technology to a high level of confidence in the ability of the systems management of the network and the individual participants to manage security and regulatory compliance risks.

1.2 The Governance Of MDLs - Does ‘One Size Fit All’?

A Mutual Distributed Ledger is a database that is consensually shared and synchronized across a network. The database is spread across multiple sites, institutions or geographies. Each user can own an identical copy. Any changes or additions to the ledger are reflected by nodes (see box 2) and copied to all participants in a matter of seconds or minutes.

MDLs can be permissionless or permissioned. Permissionless MDLs do not require registration with a central party. Users are anonymous. Permissioned MDLs require the identity of users to be whitelisted or blacklisted through some type of Know Your Customer (KYC) procedure.

Both permissioned and permissionless MDLs require a process by which the MDL is extended each time a new block of data is added.

This process must abide by the following rules:

- Data added to the MDL must maintain the integrity of the MDL structure.
- Updates must be fluid, with new data broadcast quickly to all users of the MDL.

⁷ Estonia 2016 “E-Government in Practice” <http://ega.ee/wp-content/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf>

⁸ O'Connor C. 2017 “What blockchain means for you, and the Internet of Things” <https://www.ibm.com/blogs/internet-of-things/watson-iot-blockchain/>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

- The process must be resilient to downtime and take account of individual users being unable to access the system.
- Where a discrepancy occurs between versions of the MDL broadcast by different nodes (a 'fork'), there is a process to ensure that the situation is resolved quickly and the integrity of the MDL data is maintained.

Box 2 The Significance Of Nodes

Arthur C Clarke states that *“any sufficiently advanced technology is indistinguishable from magic”*¹. What is often forgotten with MDLs, particularly when they are used for crypto-currencies, is the sheer quantity of hardware required to make them operate.

Within MDL networks transactions are added to the database in blocks, and each block is reviewed by nodes. These dedicated servers must reach a majority consensus that the block only contains valid transactions before it is added to the database. This network should be autonomous, and not require a controlling or regulating entity.¹

In the Public MDLs which are used for crypto-currencies, setting up and running a node is a voluntary activity. For some crypto-currencies, such as Bitcoin, the number of nodes on their networks is falling, causing concern.

For an MDL network to be secure, it should have a large number of independently operating nodes. If a single entity controls more than 51% of the nodes in a network, it can revise transaction history and prevent new transactions from confirming. A low number of nodes make this type of attack more feasible.

Un-permissioned MDLs assign the right to update the MDL either by Proof of Work (PoW) or Proof of Stake (PoS). There is considerable debate amongst the crypto-currency community as to the best approach.

Proof of Work requires users to find a solution to a complex mathematical problem. The more computing power a user employs, the more likely is the user achieve the solution before others and hold the right to update the MDL. In crypto-currencies such as Bitcoin, this is termed 'mining'. The first user to find a solution receives a prize of newly minted coins, which is the economic driver for participation in the process. However, mining is time intensive and carries a heavy overhead in terms of energy and equipment.

'Proof of Stake' is an alternative approach, currently used by Ripple and being explored by Ethereum. 'Proof of stake' 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 participate in the next update of the MDL.

Permissioned MDLs have different technical and governance models for achieving consensus. The choice of mechanism will depend on the deployment of MDLs and the number of active users:

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

- ◆ Regulated environments demand a ‘user of last resort’. This entity would maintain a current copy of the MDL and contracts so that it can be rebroadcast if necessary.
- ◆ A single central party could have the right to validate and update the MDL, though it is more likely that governance would require some full participants based on selection of MDL technology in the first place,
- ◆ A voting system can be established allowing users to decide on the correct version of the MDL. This requires either unanimity or a threshold number of participants.

Many other models are possible, but any ‘democratisation of data’ raises issues of governance and risk which must be addressed.

For the purposes of this report MDLs have been divided into four distinct categories: public, state-sponsored, private, and consortium.

Public MDLs are ‘permissionless’ ledgers. Crypto-currencies typically run on public MDLs. Public MDLs are designed to eliminate third parties in transactions by setting up peer-to-peer networks. Examples include Bitcoin, Ethereum, Monero, Dash, Litecoin and Dogecoin.

The original design goal of ‘permissionless’ consensus networks sought to avoid censorship and counterparty exposure. ‘Permissionless’ consensus networks allow open membership globally. They are stateless and operate beyond the jurisdiction of governments or regulators, which is why they have been described as Libertarian.⁹

Libertarianism, whose philosophy can be summed up as “The best Government is that which governs least”¹⁰ can trace its roots back to John Locke’s 1690 “Essay Concerning Human Understanding”. While modern libertarian philosophy covers a broad spectrum of political views (both left and right wing¹¹) on maximisation of individual liberty and the limits of state action, Libertarians are united in their belief in the absolute nature of property rights and the immorality of government interference in these rights. This world view can pose some interesting challenges when considering appropriate governance mechanisms. The stakeholders will view governance structures with suspicion and may resist any attempt to formalise governance of the network.

State-Sponsored MDLs are MDLs which have been established by state or state licenced bodies to deliver state sanctioned functions. These may include identity, health records, criminal records, and land registries. State-sponsored MDLs are most likely to be ‘permissioned’ systems, whereby transactions are validated and processed only by those who are already recognised by the ledger. A broader audience may be permitted to view data, based on the specific rules of the ledger. Estonia provides an excellent example of the use of state-sponsored MDLs for public service delivery through e-Estonia (see page 25).

⁹ Bartlett J 2016 “The crypto-libertarians using technology to undermine the nation-state”

<http://www.telegraph.co.uk/news/2016/05/24/the-crypto-libertarians-using-technology-to-undermine-the-nation/>

¹⁰ O’Sullivan J 1837 “The United States Magazine and Democratic Review” Oxford Library of Words and Phrases Vol. I Quotations

¹¹Stanford Encyclopedia of Philosophy <https://plato.stanford.edu/entries/libertarianism/>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

Private MDLs are permissioned commercial MDL networks, established to serve the needs of businesses. Private MDLs are by definition ‘permissioned’. The parties conducting the transactions involved must disclose their identity. MONAX, Multichain, the Hyperledger project from the Linux Foundation, R3CEV’s Corda, and the Gem Health network are examples of private blockchain projects under development

Consortium MDLs share many of the features of private MDLs, such as identity disclosure. Responsibility for the operation and maintenance of the MDL is ceded to a consortium of enterprises. Examples include the Energy Web Foundation (a global non-profit organization focused on accelerating blockchain technology across the energy sector) and the Blockchain Insurance Industry Initiative (B3i), which was launched in October 2016 to explore the potential use of distributed ledger technology in the insurance sector.

Each type of MDL presents different governance challenges. The common theme is the users’ need to have absolute confidence that the MDL network is well-run so that neither data nor assets could be lost or changed due to malfeasance, fraud, theft, coding errors, or arbitrary rule changes.

1.3 What Are The Governance Challenges Facing MDLs?

Governance is the process of interaction and decision-making among the members of any community of interest addressing collective problems, which leads to the creation, reinforcement, or reproduction of social norms and institutions.¹² Governance is the means by which those with responsibility for an organisation or a particular function within it, direct, monitor, and evaluate its work towards stated objectives.¹³ “*Good Governance : A Code for the Voluntary and Community Sector*” (second edition 2010)¹⁴ provides 6 key principles of good practice:

1. Understanding your role.
2. Ensuring delivery of organisational purpose.
3. Working effectively, both as individuals and as a team.
4. Exercising effective control.
5. Behaving with integrity.
6. Being open and accountable.

In reference to political governance (the institutions, processes, systems, rules, and laws that enable government) or corporate governance (the processes used by corporations to

¹² Hufty, M 2011 “*Investigating Policy Processes: The Governance Analytical Framework (GAF)*”. Research for Sustainable Development: Foundations, Experiences, and Perspectives Hurni, H. et al. (eds) Bern.

¹³ Harris I, Mainelli M and Critchley S 2001 “*Information Technology Governance In The Not-For-Profit Sector: An ICSA Best Practice Guide*” <http://www.zyen.com/37-publications/professional-articles.html?type=rss&start=165>

¹⁴ The Code Steering Group 2010 “*Good Governance A Code for the Voluntary and Community Sector*” (second edition)

Responsibility Without Power? **The Governance Of Mutual Distributed Ledgers**

make decisions), governance may be considered as the application of a common set of structures and tools designed to facilitate group decision-making.

The fundamental premise of MDLs is that no single entity or interest group should have full power over the MDL. Control should be decentralised. Even for private MDLs, control demands that the platform owners providing access cannot change the data on the MDL itself.¹⁵ Conceptually, the structures are embedded in code and “code is law”.¹⁶ Adopting this approach as basis for integrity and trustworthiness leads to two problems:

First, by eliminating the need to trust a third party middleman,¹⁷ traditional business dispute resolution no longer works. The common enforcement infrastructures, such as state courts or private courts of arbitration, cannot direct an intermediary, such as a bank or credit card company, to reverse a payment.¹⁸ If a dispute arises over the quality of goods or services supplied, how can aggrieved parties obtain recourse especially if each node operates under the laws of its own physical jurisdiction?

Second, particularly for crypto-currency networks, public MDLs can only be trustworthy when no single entity or interest group controls more than 50% of the nodes. That would enable them to change the data. Users must have confidence that rules are being applied correctly in the MDL software.

To establish confidence, MDL founders must answer the following questions:

1. Who is providing the software and to whom are they accountable?
2. How is transparency ensured?
3. How are security and confidentiality ensured across the network?
4. How are decisions scrutinised, and how is the performance of the MDL managed?

1.4 How Should MDL Governance Structures Be Organised?

The basis of most governance is a two-tier structure. A small group of individuals are responsible for running an organisation or project, for example a board of directors or project management committee, but are accountable to a wider group of individuals, often called stakeholders or members.

Satoshi Nakamoto’s original vision for crypto-currencies was for a flat governance structure, resembling a collective. This structure is characterised by attempts to share and exercise political and social power. Collective structures enable decision making on a consensus-

¹⁵ Beehive 2017 “When is a blockchain not a blockchain?” <http://blog.beehive.ae/when-is-a-blockchain-not-a-blockchain/>

¹⁶ Lessig L 2006 “Code V.2.0” Basic Books ISBN 144299648X

¹⁷ Nakamoto S 2009 “Bitcoin open source implementation of P2P currency” <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>

¹⁸ Oermann M and Töllner N 2015 “The Evolution of Governance Structure in Cryptocurrencies and the Emergence of Code-Based Arbitration in Bitcoin” https://publixphere.net/i/noc/page/IG_Case_Study_Bitcoin_and_Autonomous_Systems

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

driven and egalitarian basis,¹⁹ which is “high in participation, low in definition”²⁰. In practice, any group of people that comes together for any length of time for any purpose will form an organisational structure.²¹ By avoiding the creation of formal governance structures, ‘elites’ will emerge. An elite is a small group of people who have power over a larger group of which they are part but, usually without direct responsibility to that larger group, often without their knowledge or consent.

Governance structures evolve to suit the purposes of an organisation or project. They generally demonstrate one of the following five archetypes:²² (see glossary for an explanation of terms).

- 1) **Oligarchy:** The board is composed by the members and stakeholders. New appointments to the board are made by the board. This is a common structure for the voluntary sector or charitable organisations.
- 2) **Appointed board:** Board members may or may not be members of the organisation and are appointed by stakeholders or the board itself to bring a particular set of knowledge and skills to the table. The appointment of non-executive directors is a good example of this.
- 3) **Representative:** This is a model for organisations that wish to have enterprises rather than individuals as members, such as trade, business or governmental institutions. Each organisation appoints an individual to serve on the board. A version of this model can also be used for 'joint ventures' where two or more organisations wish to establish a legal form, in order to run a project together. Each 'owner' of the new legal form has the right to appoint an individual to the board.
- 5) **Membership:** This model ensures that a number of individuals or organisations have rights in relation to a project or programmes. It is a democratic structure. Board members are elected to their positions and tenure is for a fixed period of time.
- 6) **Co-operative:** The International Co-operative Alliance (ICA) Statement on Co-operative Identity describes a co-operative as ‘an autonomous association of persons united voluntarily to meet their common economic, social and cultural needs and aspirations through a jointly owned and democratically controlled enterprise’.²³ One key feature is 'one member one vote'.

¹⁹ Anon 1971 “*Anti-Mass: Methods of Organization for Collectives*”

https://ia902608.us.archive.org/5/items/Anti-massMethodsOfOrganizationForCollectives/anti_mass.pdf

²⁰ McLuhan M & Lapham 1994 “*Understanding Media: The Extensions of Man*” MIT Press 2nd Edition ISBN 153743005X

²¹ Freeman J 1971 “*The Tyranny of Structurelessness*” <http://www.jofreeman.com/joreen/tyranny.htm>

²² NCVO 2017 “*Working out your Governance Structure*” <https://knowhownonprofit.org/basics/setting-up-a-charity/getting-your-charity-started/governance-structures>

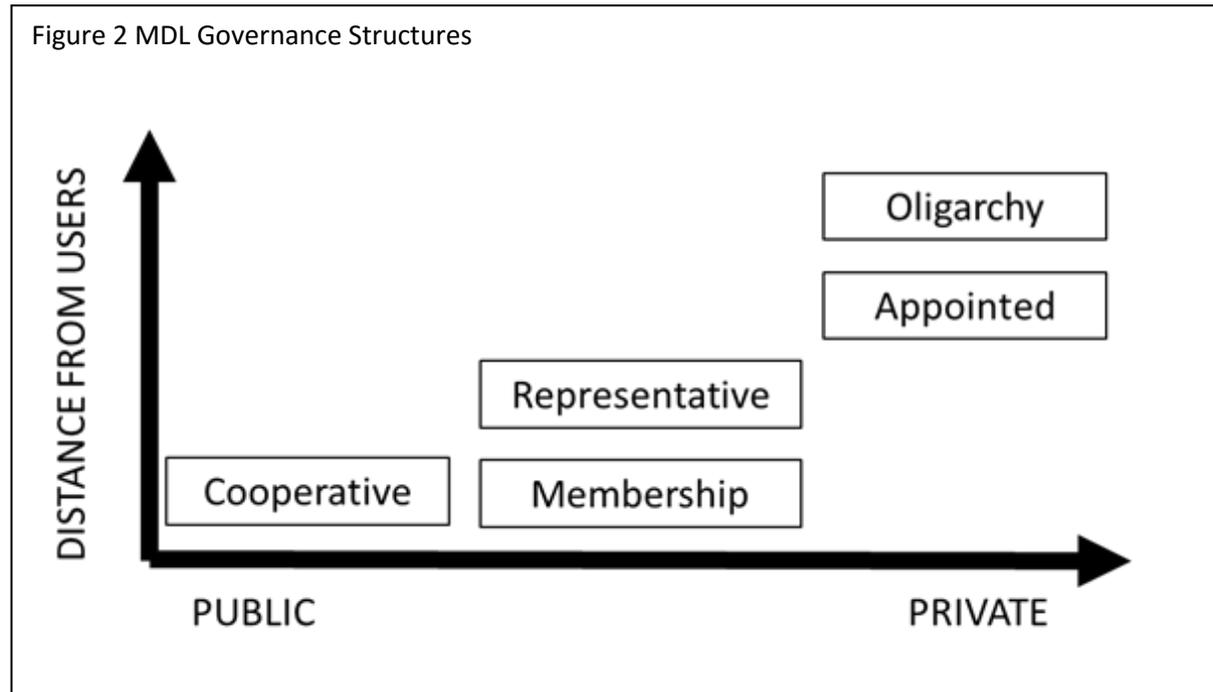
²³ ICA 2017 “*Co-operative identity, values & principles*” <http://ica.coop/en/whats-co-op/co-operative-identity-values-principles>

Responsibility Without Power?
The Governance Of Mutual Distributed Ledgers

The most appropriate structure for governance depends on the form and function of the network (see table 2), and the proximity of users to the governance structures (see Figure 2):

Table 2 MDL Use Classes And Their Corresponding Governance Structures

Type of MDL	Use Class	Governance Structure
Un-permissioned	Public MDLs: Little formal governance structure. <i>E.g. Crypto-currencies</i>	Co-operative: An autonomous association, jointly owned and democratically controlled.
Permissioned	State sponsored MDLs: Governance structures of sponsoring agencies grafted on. <i>E.g. land registries or identity</i>	Appointed Board: Board members are appointed by stakeholders, or the board itself, to bring particular knowledge and skills to the table.
Permissioned	Private MDLs: Highly defined governance structure. <i>E.g. platforms for blockchain-based applications for business ecosystems.</i>	Oligarchy: The individuals that comprise the board are the owners or stakeholders.
Permissioned	Consortium MDLs: Established and managed by a group of organisations rather than a single entity, likely to have a complex governance structure. <i>E.g. Financial Services or Internet of Things (IoT) platforms.</i>	Membership: Board members are elected to their positions and tenure is for a fixed period.
Permissioned	State-Sponsored and Consortium MDLs (see above)	Representative: For organisations that wish to have members who are enterprises instead of individuals. This structure may be appropriate for both consortium and state-sponsored MDLs.



1.5 The Architecture Of Governance

In most organisations, governance operates at three levels:

1. **Market Governance:** the system of regulations and social norms within which organisations operate. This is external to the organisation and the organisation may or may not be able to influence it.
2. **Corporate Governance:** the system of rules, practices and processes by which goals are set, stakeholder expectations met, strategies developed and risk and compliance managed.
3. **Project Governance:** the policies, regulations, functions, processes, procedures, and responsibilities that define the establishment, management, launch and control of projects, programmes and portfolios.

Internally, most organisations operate hierarchical systems of governance. Some governance structures may be recursive, through subsidiary boards which are established to focus on particular elements of systems or processes.

In complex, multi-lateral projects, governance structures require joint working committees and delivery teams. The committees and teams will have to be incorporated in the governance structures of the cooperating enterprises.

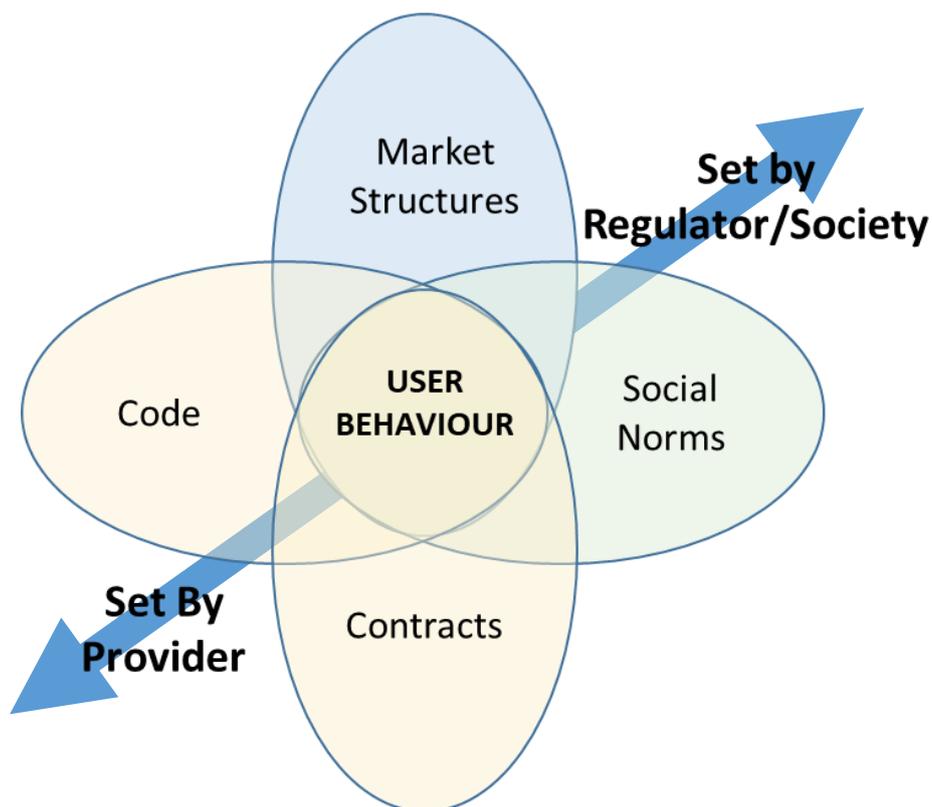
The architecture of governance structures within an MDL depends on the use it is being put to and the number of users. Within MDLs, stakeholder, user and customer behaviour is constrained by four factors (see figure 3):

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

1. The legal framework that enables commercial activity to take place.
2. The social norms, including security considerations, under which the network operates, namely the code behind the MDL and the contracts developed to run on it.
3. The code that governs interaction within the network.
4. The contracts that define relationships between users.

The first two of these are determined by outside forces. The use of MDLs by businesses, particularly the financial services sector, requires the outside forces remain a material consideration. By contrast crypto-currencies were specifically established to circumvent legal frameworks and social norms. Market structures and social conventions (such as ethics) lie outside scope of MDLs, but the management of the remaining two factors require governance.

Figure 3 Model Of Governance Factors In MDLs



Adapted from Oermann *et al* 2014²⁴

²⁴ Oermann M *et al* 2014 "Approaching Social Media Governance" HIIG Discussion Paper Series, (May 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2498552

1.6 The Role Of Trust In Trustless Systems

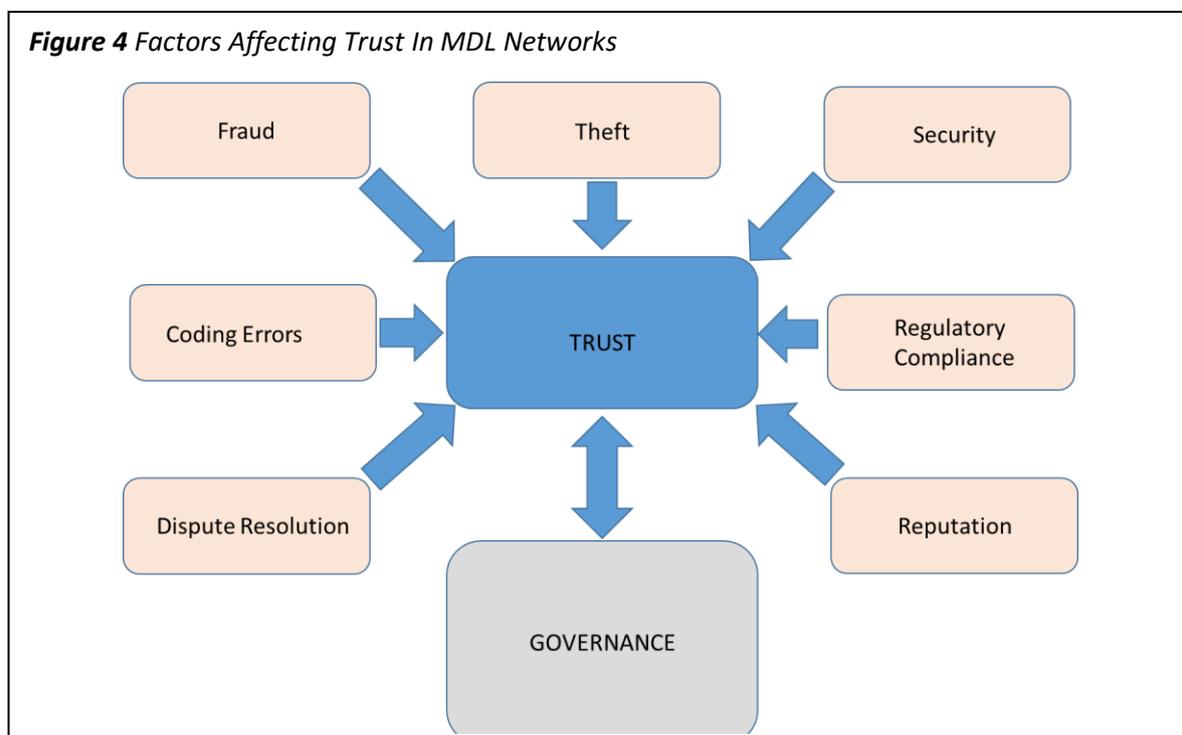
Despite being described as ‘trustless systems’ (see box 3), the foundations of MDLs are built on trust:

1. Trust in the code that supports the protocols for the network and ‘smart contracts’.
2. Trust that transactions will not be lost due to a ‘hard fork’, ‘soft fork’ or ‘roll back’ (see Glossary).
3. Trust in the algorithms that protect security and privacy.
4. For crypto-currencies, trust that other users will continue to believe in the future persistence of community valuation of a ‘virtual element’.

The description of MDLs as ‘trustless systems’ is inaccurate. MDLs reassign trust. Instead of trusting laws and institutions, users are expected to have confidence in other stakeholders, programmers, and those who are technically accomplished enough to be able to verify the code. *“We aren’t actually trusting the blockchain technology; we are trusting the people that support the blockchain”.*²⁵

Cryptographers define something ‘trusted’ as something that you are vulnerable to.

The value of an MDL network to its users is often proportionate to the number of users participants. When the number of participants in an MDL network grows, all stakeholders benefit. If trust in an MDL is eroded the number of users will decrease and the value of the network to the remaining users is diminished. A number of factors influence levels of trust in MDLs (see figure 4).



²⁵ Spode E 2017 “The great cryptocurrency heist” <https://aeon.co/essays/trust-the-inside-story-of-the-rise-and-fall-of-ethereum>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

The degree to which the factors in figure 4 impact on trust depends on how well the system is governed. Good governance lies at the heart of all successful organisations and institutions. Good governance is critical to protecting organisations from poor decisions and exposure to dangerous risks. Therefore, a decision-making process that incorporates good governance attributes will produce better policy outcomes.²⁶

Box 3 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.

Trust is not required for transactions on MDLs, which is why they are sometimes referred to as 'trustless systems'.

1.7 Ethics And Social Norms

Ethics systematises, defends and recommends concepts of right and wrong conduct. Issues of ethics are based on perception and social norms rather than legal certainty.

Private and consortium MDLs, where members are identifiable and known to each other, use a teleological approach. Ethics focussed on legal positivism (law based on getting the right outcome²⁷) and bound into service level agreements, is likely to be the favoured approach.

For state-sponsored MDLs issues around privacy and the use that data is put to, are likely to be the primary ethical consideration (see section 2.3). Public MDLs face the biggest ethical challenge given the diversity and anonymity of their users.

Do MDLs have an obligation to police the use of the platform? Many forms of crime, such as money laundering, human trafficking, extortion, child pornography, tax evasion, and payment for criminal services can be facilitated using MDLs.

²⁶ ICAEW 2013 "What should companies be responsible for? What We Think: A Dialogue In Corporate Governance" <http://www.icaew.com/-/media/corporate/files/technical/corporate-governance/dialogue-in-corporate-governance/icaew-tl-g1-web.ashx?la=en>

²⁷ Harris I 2008 "Commercial Ethics, Process Or Outcome?" Gresham College Lecture <http://www.zyen.com/Activities/Events/Gresham%20College%20Commercial%20Ethics%20-%20Process%20or%20Outcome%20-%20Published%20Transcript%20Including%20Slides.pdf>

Social media platforms have been forced into policing crime committed through platforms.²⁸ Unlike MDLs, social media platforms have control over the content which they publish. No ready-made solutions present themselves but public MDLs must give consideration to the construction and enforcement of ethical frameworks for acceptable use within their networks. If a public MDL decides to adopt a constitution (see section 2.2) it must bind both its governance structures and its users.

1.8 Market Structures And MDLs

Contract law facilitates exchange of goods and services for consideration. In theory, the permanent, persistent, and pervasive nature of MDLs should simplify the market governance structures required for exchange. Counterparties in a trade are able to demonstrate verified, time stamped transactions, reducing the possibility of fraud or dispute.

Not all contracts fit comfortably under this model.²⁹ Long-term contracts and contracts, where there is significant uncertainty (particularly insurance) demand flexibility. Third parties may be required to resolve disputes through arbitration, mediation, expert determination and other governance structures.

Two separate technological solutions may reduce uncertainty in this area:

- **Ricardian Contracts** – A Ricardian Contract can be defined as a single document that is:
 - a) A contract offered by an issuer to holders.
 - b) For a valuable right held by holders, and managed by the issuer.
 - c) Easily readable by people (like a contract on paper).
 - d) Readable by programs (parseable like a database).
 - e) Digitally signed.
 - f) Self-contained with respect to the keys and server information, and.
 - g) Allied with a unique and secure identifier.³⁰

In other words, a Ricardian contract is a digital contract that contains all terms and clauses of a legally conventional written contract but it is readable both by people

²⁸ Brown N 2017 "Should Social Networks Be Held Liable for Terrorism?"
http://www.slate.com/articles/technology/future_tense/2017/06/a_new_legal_theory_for_holding_social_networks_liable_for_terrorism.html

²⁹ Macneil I 1987 "Contracts: Adjustment of Long Term Economic Relations Under Classical, Neo-Classical and Relational Contract Law" 72 Nw. U. L. Rev. 854 (1977-1978)
<http://heinonline.org/HOL/LandingPage?handle=hein.journals/illlr72&div=46&id=&page=>

³⁰ Grigg I 2000 "Financial Cryptography in 7 Layers" 4th Conference on Financial Cryptography,
<http://iang.org/papers/>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

and by software.³¹ The document is digitally signed, to prove authenticity and a unique and secure identifier (or hash) is generated to enable it to be embedded into all transactions. Originally developed by Ian Grigg and Gary Howland as part of the Ricardo payment system, Ricardian contracts allow parties the opportunity to define in full the meaning of their transactions, and to lock in that meaning to the transaction.

- **Multi-Signature Transactions** – An MDL can set authorisation conditions to approve user transactions. One approach requires two parties to approve any given transaction. This enables a third party arbitrator to be nominated. If a transaction proceeds smoothly, both parties can sign, enabling the transaction to go be completed. Where one party withholds their signature, the nominated arbitrator can determine whether the transaction is valid then grant or withhold approval. The arbitrator appends their signature for valid transactions to proceed. Where they determine a transaction is invalid, they withhold their signature. The transaction is void. This model could be used for any MDL platform. Financial services transactions would require the third party to be registered with a financial regulator and potentially responsible for AML due diligence.³²

Arbitration may be required when disputes arise. A clear pathway for dispute resolution will enhance trust in MDL networks. Potential ways of doing this include:

1. **Community determination** - where a network uses majority consensus to rule on a dispute.
2. **Expert determination** - where an independent third party makes a final and binding determination in a dispute.
3. **Mediation** - a 'without prejudice' process that helps both parties reach a resolution, yet often takes into account how a court might have interpreted the situation.
4. **Arbitration** - dispute resolution by a third party, effectively an arbitrator similar in function to an arbitrator for complex international conflicts for parties requiring speedy resolution of the dispute.

One solution for disputes arising as a result of Ricardian or smart contracts (see box 4) is the development of a standard set of interpretation/dispute resolution rules. The model is similar to the arbitration rules promulgated by forums such as The London Court of International Arbitration (LCIA), International Chamber of Commerce (ICC) and The International Centre for Settlement of Investment Disputes (ICSID), which could be incorporated by distributed ledger designers.

Arbitration bodies could examine the opportunities to adapt their rules for MDLs by establishing a regular panel of expert coders/DLT experts. The experts could publish

³¹ Simoyama et al 2017 "Triple entry ledgers with blockchain for auditing" Int. J. Auditing Technology

³² FCA 2015 "Financial crime: a guide for firms Part 1: A firm's guide to preventing financial crime"

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

opinions on issues which frequently arise and propose procedures to address them. The solutions could form a discrete set of standards for developers to incorporate into Ricardian or smart contracts.

Provision of a set of standards is a straight-forward exercise for private or consortium MDLs. Users are bound by contracts and terms of use agreements. This solution may not be satisfactory for public MDLs because users may be anonymous or located in different jurisdictions. Enforcement of arbitration decisions will be more complex unless effective governance mechanisms are in place.

Box 4 Smart Contracts

A smart contract is *“the implementation of contract terms as executable computer code”*.¹ A simple example of a smart contract is a weather derivative contract which pays \$50,000 on every day in July when the temperature recorded by a given field on the Met Office website is above 33 °C.

A smart contract is neither smart nor a contract. It is a code element containing two basic components:

- a) Conditions which trigger action(s) – temperature of 33 °C, and,
- b) Actions to execute – pay \$50,000.

Smart contracts can be powerful tools for dis-intermediating simple transactions and making administration and processing swifter, more efficient, and more accurate. However, any error in the underlying data may result in an incorrect contractual outcome from execution of code, for example triggering an incorrect transfer of assets.

Part 2 Governance Structures For MDLs

2.1 Introduction

Effective governance structures for MDLs are necessary. Failures, caused by exceptions, malfeasance, rent-seeking (attempts to increase personal profit by manipulating redistribution of resources rather than creating new wealth), or unjust enrichment undermine confidence in trustless systems. This section explores the challenges facing different types of MDL.

2.2 Governance Structures For Public MDLs

The key governance challenges facing a public MDL are:

- ◆ The anonymity of the users, which complicates dispute resolution and enforcement across jurisdictions.
- ◆ The lack of agreed ethical standards for users or the means to enforce them, which facilitates criminal and malicious use of the MDL.
- ◆ The lack of an agreed formal framework and structure for governance, which calls into question the legitimacy of code changes and hinders strategic planning and risk management.

Public MDLs provide a platform that users can access to conduct transactions without charge.

Other free service providers, who faced similar issues, can be used as examples in order to identify potential solutions to these challenges. A good example is Gmail, the free email service developed by Google.

Gmail requires users to agree to its terms and conditions. The terms and conditions include prohibitions on the use of the service for malicious or criminal activity. Their definition of criminal activity includes the State and Federal Laws of the United States, and the jurisdiction of the user. Where Google is made aware of a breach of these terms and conditions, they can suspend or terminate the service.

Public MDLs are not corporations but decentralized consensus systems, which are based on peer-to-peer principles rather than central authority³³. They can be viewed as ‘communities’ and defined as self-organised networks of people with a common agenda, cause or interest, who collaborate by sharing ideas, information, and other resources.³⁴

³³ Glaser F & Bezenberger L 2015 “Beyond Cryptocurrencies - A Taxonomy Of Decentralized Consensus Systems” 23rd European Conference on Information Systems
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605803

³⁴ Business Dictionary *Definition of Community*
<http://www.businessdictionary.com/definition/community.html>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

As discussed in section 1.4, communities have a tendency to self-organise. A good example of this can be found in the response to the March 2013 accidental fork of bitcoin³⁵. The split was detected very quickly, and because the right people were online or could be contacted directly, decisive action was taken promptly.

According to the model in Figure 2 (page 17), public MDLs lend themselves to a cooperative model of governance. Cooperatives are defined by their adherence to a rigid constitutional structure³⁶ requiring governance to be carried out in the interest of their stakeholders.

A constitution is a body of fundamental principles or established precedents, according to which a state or other organisation is acknowledged to be governed.³⁷ A constitution can embody terms of use and policies which bind users to a code of conduct. The code of conduct comprises ethical terms and dispute resolution. A constitution can also define the governance structures.

The development of a constitutional approach to public MDL governance must consider legitimacy, as decisions will apply to all stakeholders.³⁸ The constitution must define the stakeholders for public MDLs and representation of their interests. By way of illustration in crypto-currencies, the principal stakeholders comprise:

1. **Miners** – the creators of blocks.
2. **Developers** – the creators of the code that underlies the system.
3. **Nodes** – the hardware that broadcast messages across a network as the first step in the transaction process which results in a block confirmation.
4. **Users** – the individuals or organisations transacting in crypto-currency.

Effective constitutional governance requires Montesquieu’s separation of powers,³⁹ notably the separation of judicial power from executive and legislative (see table 3).

Table 3 Analysis Of Power Functions Within Crypto-currencies

Branch of Power	Purpose	Crypto-currency Equivalent
Legislative	Enacting policy and laws and appropriating the resources necessary for governance.	Developers – ‘Code as law’.

³⁵ Narayan A 2015 “Analyzing the 2013 Bitcoin fork: centralized decision-making saved the day” <https://freedom-to-tinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork-centralized-decision-making-saved-the-day/>

³⁶ Cooperatives UK “Model Governing Documents” <https://www.uk.coop/developing-co-ops/model-governing-documents>

³⁷ Oxford English Dictionary Definition of constitution in English <https://en.oxforddictionaries.com/definition/constitution>

³⁸ Wikipedia Politics <https://en.wikipedia.org/wiki/Politics>

³⁹ NCSL “Separation of powers- an overview” <http://www.ncsl.org/research/about-state-legislatures/separation-of-powers-an-overview.aspx>

**Responsibility Without Power?
The Governance Of Mutual Distributed Ledgers**

Executive	Implementing and administering the policy and laws enacted and funded by the legislative branch.	Miners – Choosing to accept, reject, or fork.
Judicial	Interpreting policy and laws and applying (and enforcing) interpretations to exceptions.	No equivalent.

Analysis of the power functions within crypto-currencies would conclude that there is no judicial element. The interests of users and nodes are not currently represented. The health of MDL ecosystems is likely to benefit from the adoption of constitutions. Constitutions must clearly define:

- ◆ The terms of use of the MDL.
- ◆ How stakeholder interests are represented.
- ◆ How code changes can be made.
- ◆ How judicial functions will be exercised.

A variety of processes have been created to deliver effective governance outcomes. Two are illustrated below:

1. **Open processes.** These are best illustrated by the example of the Internet Society, an American, non-profit organization founded in 1992 to provide leadership in Internet-related standards, education, access, and policy⁴⁰. The Internet Society is governed by a board of trustees and supports and promotes the work of the standards settings bodies for which it is the organizational home. These bodies include the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), and the Internet Research Task Force (IRTF). These bodies are organized into working groups and informal discussion groups, each dealing with a specific topic. Each working group has an appointed chairperson, along with a charter that describes its focus, and what and when it is expected to produce. They are open to all who want to participate, and hold discussions on an open mailing list or at meetings. An open and inclusive approach confers legitimacy on decisions and policy creation. However, the processes are slow and decisive action to counter immediate threats is difficult.
2. **A structured approach.** These can be delivered through a Foundation. Foundations are not for profit organisations that use their income to fund or otherwise support other organisations or individuals. In their 2002 report “Evidence of Worth”⁴¹, Mainelli, Harris and O’Callaghan identify the types of goals for not for profit organisations.

⁴⁰ The Internet Society 2017 “Who We Are” <https://www.internetsociety.org/development>

⁴¹ Mainelli M, Harris I and O’Callaghan M 2002 “Evidence of Worth” Journal of Strategic Change, Volume 11, Number 8, John Wiley & Sons (December 2002) pages 399-410.

Responsibility Without Power?

The Governance Of Mutual Distributed Ledgers

- ◆ Expanding frontiers to mitigate needs (e.g. a medical charity developing drugs which might cure and/or prevent disease).
- ◆ Changing systems to remove or release needs (e.g. an advocacy organisation seeking to change government policies).
- ◆ Service delivery to meet needs (e.g. a UK charity providing care homes for the elderly).
- ◆ Communitarian to address needs for or through community activity (e.g. a volunteering organisation, a trades union or a professional institute).

A foundation established to support an MDL is likely to focus resources on service delivery and communitarian goals. In order to deliver effective governance for a public MDL the constitution of a Foundation must:

- ◆ Define how governance decisions are made. If governance is the responsibility of a board of directors or trustees, the appointment mechanism should be clarified. Their roles and responsibilities should be clearly established. Their ability to delegate any of their powers or functions should be outlined.
- ◆ Outline oversight and reporting arrangements.
- ◆ Establish how stakeholder engagement will be maintained. If this is moderated through user groups and advisory working groups, the way they inform the work of the board of directors or trustees should be clearly established.
- ◆ Establish an independent mechanism for dispute resolution which has the power to enforce decisions.
- ◆ Establish the terms of use that users must accept in order to access the service.

Constitutions are a prerequisite for the effective governance of public MDLs.

2.3 Governance For State-Sponsored MDLs

The key governance challenges facing a public MDL are:

- Ensuring that the MDL is integrated into the governance structures of the sponsoring department.
- Ensuring effective engagement with key stakeholders, including other departments which will be affected by the MDL.

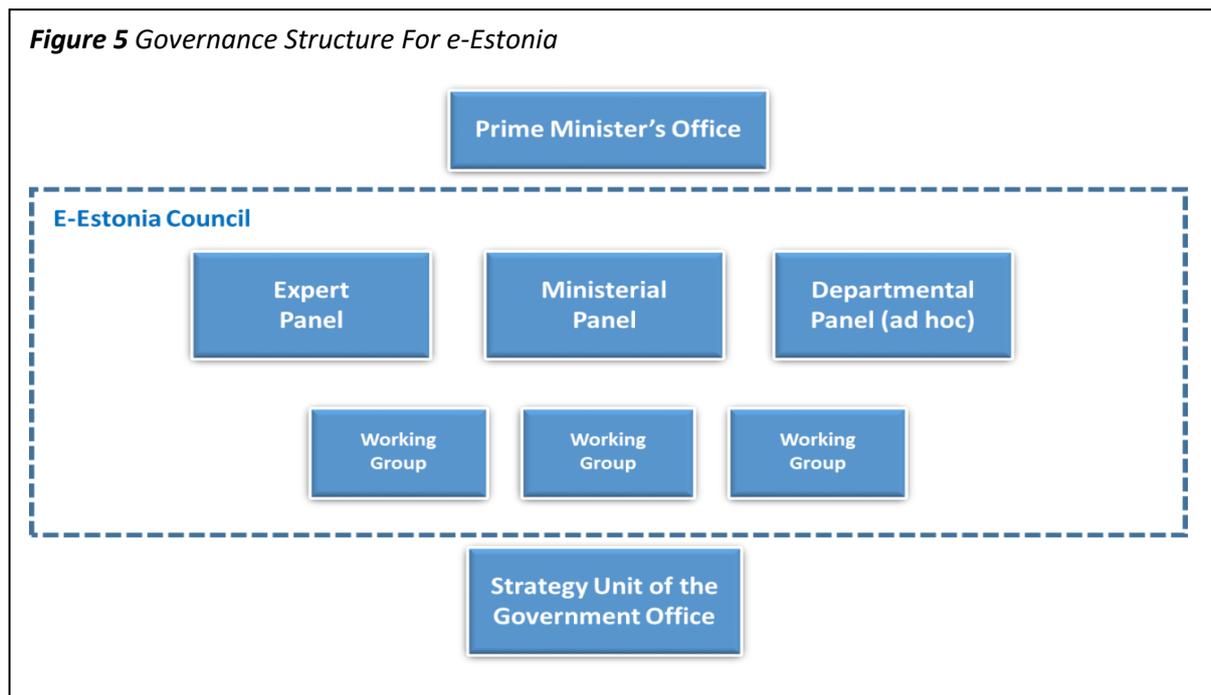
Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

- Ensuring that oversight is carried out by individuals with the knowledge and skills required to understand the code, the risks and the performance criteria for the MDL.

A number of trials throughout the world are using MDLs to provide state functions, including land registries, welfare benefits, and healthcare records.⁴² MDLs hold particular promise in the field of identity.

Estonia is acknowledged as a leading nation in the adoption of blockchain technology. Estonia citizens and e-residents are issued a cryptographically secure digital ID card powered by blockchain infrastructure, allowing access to various public services.⁴³

The governance model for the majority of countries trialling the use of MDL systems is for the ledgers to be grafted onto project boards within the governance structures of the sponsoring agencies. In Estonia, the *e-Estonia Council* has been established as an adjunct to the Prime Minister's Office to coordinate the development of Estonian digital society and e-governance, specifically the implementation of the national digital agenda.⁴⁴ The *e-Estonia Council* establishes expert committees and working groups and commissions studies in the field of ICT policy (see figure 5).



⁴² Kwang T 2017 "How are governments using blockchain technology?"

<https://www.enterpriseinnovation.net/article/how-are-governments-using-blockchain-technology-1122807855>

⁴³ Shen J 2016 e-Estonia: "The power and potential of digital identity"

<https://blogs.thomsonreuters.com/answeron/e-estonia-power-potential-digital-identity/>

⁴⁴ Estonia 2016 "e-Governance in Practice" <http://ega.ee/wp-content/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

Privacy is a concern when considering pervasive, universal, or state identity schemes.⁴⁵ A right to privacy is a key feature of both the Universal Declaration on Human Rights and the European Convention on Human Rights. The right to privacy may be expressed as “a person’s right to control access to his or her personal information.”⁴⁶

The European Data Protection Directive 95/46/EC,⁴⁷ the forthcoming General Data Protection Regulation (GDPR),⁴⁸ and the UK Data Protection Act 1998 contain some useful principles for consideration in the governance of MDLs:

1. Data should be held for legitimate purposes. Personal data should be obtained only for specified purposes. It should not be shared with other agencies, nor processed further without the express permission of the individual that data concerns.
2. Data should be transparent. People should be able to know data retained on their identity. They should be able to correct the data if there are errors and understand how their data is used in reaching decisions that affect them.
3. Data should be proportional. Data held on individuals by a third party should be proportional and relevant for the purpose intended.

Article 12 of the Directive 95/46/EC the EU gave a legal base 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 only (May 30, 2014), Google received in excess of 12,000 requests to have personal details removed from its search engine. The persistent nature of MDLs will require careful thought for this kind of legislation

The use and retention of ownership of personal data through public and private keys held by individuals provides one possible solution to the governance of privacy in MDL systems. Public and private key cryptography involves two uniquely related cryptographic keys. The private key is held by an individual who can use it to encrypt documents, send them, along with a copy of the public key, to people or organisations with whom they wish to share data. The public key can be used to encrypt documents to be signed and returned. Those documents will, in turn, only be accessible through the use of the private key.

⁴⁵ Martin A and Martinovic I 2016 “*Security and Privacy Impacts of a Unique Personal Identifier*” Cyber Studies Programme, Working Paper No. 4 University of Oxford
<https://www.politics.ox.ac.uk/materials/publications/14987/workingpaperno4martinmartinovic.pdf>

⁴⁶ Duhaime's Law Dictionary “Privacy legal definition”

<http://www.duhaime.org/LegalDictionary/P/Privacy.aspx>

⁴⁷ Data Protection Directive 95/46/EC <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3A114012>

⁴⁸ Allen and Overy 2017 “*GDPR Guide*”

<http://www.allenoverly.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf>

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

Individuals can use a private key to upload documentation (such as birth certificates, social security numbers, passports, or healthcare information) to an MDL. Where individuals have to share that information with an agency, they can provide a copy of their public key for time-limited access.⁴⁹

Jurisdictions have different attitudes to sharing personal data.⁵⁰ The governance of privacy and personal data is a critical consideration in the governance of state-sponsored MDLs.

Box 5 Smart Contracts, a Potential Solution to the Issue of Privacy?

Privacy is not just a concern for state-sponsored MDLs. Privacy regulations have a significant impact on commercial organisations, where the trend for increasingly onerous requirements on organisations seems set to continue, notably with the implementation of the EU's GDPR legislation in May 2018.

Generally, an organisation will implement such legislation by creating or updating a policy document at Board or Risk Committee level, and then giving this to business and support units to achieve compliance.

By using the policy document (rather than a legal contract with a third party) as the starting point, smart contracts could provide a natural framework for implementing the requirements in operational processes and systems. One particular advantage of this approach is a clear audit trail of the rigour with which the organisation has complied with the legislation, thus simplifying the dialogue with the regulator.

A further advantage is that as laws and regulation change, the audit trail will assist in changing the control structure efficiently. This is in contrast to the typical circumstances today, where new controls are layered over old ones, since there is no clear understanding of what controls are implemented in the system and how they actually work.

Suppose, for example, that the policy says: *"Since each jurisdiction can have its own laws on privacy, each piece of sensitive information must have a recorded jurisdiction of origin and the management of that sensitive information must conform to the laws of that jurisdiction."* The original smart contract might contain an instruction to be executed before allowing a particular action on a particular element of sensitive information.

⁴⁹ A working example of this type of system can be found at <http://idchainz.com/>

⁵⁰ European Commission 2011 "Attitudes on Data Protection and Electronic Identity in the European Union" Special Eurobarometer 359 http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf

2.4 Governance For Private And Consortium MDLs

Private and consortium MDLs are for profit services that operate in a commercial environment. Some of the challenges that they face are very similar including:

- ◆ enhancing trust in the MDL through transparent decision making processes, supported by robust risk and performance management;
- ◆ the development of systems to manage legal compliance, resilience and security, which are implemented by all users;
- ◆ the establishment of independent dispute resolution mechanisms;

Consortium MDLs also face the additional challenges of:

- ◆ effectively managing the expectations and needs of the organisations who are part of the consortium;
- ◆ ensuring that the governance structure is independent and not unduly influence by individual organisations or factional groups within the consortium.

Private and consortium MDL networks will benefit from sound corporate governance, *“the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled within organisations. It encompasses the mechanisms by which organisations, and those in control, are held to account”*.⁵¹

Corporate governance is the responsibility of a managing board. The managing board must articulate the ambition of an organisation and to manage the risk that that ambition contains.⁵²

The relationship between the board and users can be moderated through Service Level Agreements (SLAs), contracts which define the services and the standards to be delivered.⁵³ The SLA lays out the expectations of stakeholders on service performance and the behaviours expected of users by the MDL managers. A typical SLA requires:

- ◆ Performance metrics and monitoring systems.
- ◆ Agreed sanctions and compensation levels for violations of the terms of the SLA.

SLAs provide an opportunity to prescribe agreed processes for dispute resolution for private and consortium MDLs. Although no working examples of SLAs for MDLs were found in the course of this research, their development and standardisation will be a crucial factor in the uptake of MDL technology within the commercial arena.

Managing boards of private and consortium MDLs can take the following forms:

⁵¹ Justice Owen April 2003, *“The Failure of HIH Insurance Volume 1: A Corporate Collapse and Its Lessons”*, Commonwealth of Australia, HIH Royal Commission

⁵² NLC 2009 *“The Healthy NHS Board, Principles for Good Governance”*

Responsibility Without Power?

The Governance Of Mutual Distributed Ledgers

- ◆ **Developer company managing boards**, which essentially involve the existing governance structures of the companies producing proprietary systems or services. These are more likely to resemble the oligarchy or appointed models.
- ◆ **Joint project working boards**, established to oversee multi-party collaborative MDLs. They may resemble the membership or cooperative models discussed earlier.

There are many examples of joint project working boards in the commercial arena. One example of particular relevance to consortium MDLs intended for use in the financial services sector is the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. The SWIFT system is a global messaging network designed to transfer financial messages in a secure and timely manner.

SWIFT is organised as a cooperative society owned by its members (approximately 3,500 firms from across the world), who are categorized into classes based on share ownership.

It is governed by a Board of 25 independent directors, representing banks across the world. The Executive Committee is a group of full-time employees headed by the Chief Executive Officer.

For legal compliance purposes, SWIFT does not monitor or control the messages that users send through its system. All decisions on the legitimacy of financial transactions under applicable regulations, such as sanctions regulations, rest with the financial institutions handling them, and their competent international and national authorities.

SWIFT does allow financial institutions to include underlying customer information in cover payment transactions in order to help its users in meeting their responsibilities to comply with national and international regulations.

Although SWIFT is not immune to hacking and fraud, its established governance structure and well defined policies and procedures for grievance and risk management allow for rapid and decisive action.

SWIFT is currently exploring MDL technology. SWIFT is an imperfect model for governance of a consortium MDL. For example an examination of the fee structure shows that all members of the SWIFT networks pay a one-time joining fee plus annual support charges which vary by member classes. SWIFT also charges users for each message based on message type and length and these charges vary depending upon the bank's usage volume. The dominant market position of SWIFT has led to accusations from some quarters of rent-seeking. As a result, organisations establishing a consortium MDL should pay particular attention to the foundation constitution which should define the scope of any fees.

2.5 Project Governance For MDLs

Project Governance is the management framework within which decisions on a project are made. The governance of programmes and projects is a necessary part of organisational

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

governance. Effective governance systems give organisations the required internal controls but enables compliance with stakeholder demands.

In delivering an MDL project, good project governance can be demonstrated⁵⁴ through:

1. The adoption of lifecycle governance that includes recording and communicating decisions made at decision points.
2. The acceptance of responsibility by the organisation's management board for governance.
3. Clearly defined roles, responsibilities and performance criteria for governance.
4. Procedures that allow a management board to deploy independent scrutiny of projects, programmes, and portfolios.
5. Giving delegated bodies the capability and resources to make appropriate decisions.
6. Ensuring that stakeholders are engaged at a level that reflects their importance to the organisation and in a way that fosters trust.

A consortium MDL should also develop:

1. Formally agreed governance arrangements covering unified decision-making and joint authority for managing contacts with owners, stakeholders, and third parties.
2. Jointly agreed business cases that reflect the apportionment of risk and reward.
3. Governance arrangements that take into account the existing governance structures, as well as the technical strengths and weaknesses of the co-owners.
4. Pre-agreed decision points that give the owners the opportunity to re-evaluate their participation.
5. Formally agreed procedures for corporate and risk management reporting, third-party verification, and dispute resolution.

A range of project management methodologies and standards are available to organisations seeking to formalise and monitor the governance of projects.

2.6 Does The Governance Of Legacy IT Systems Hold Lessons For MDLs?

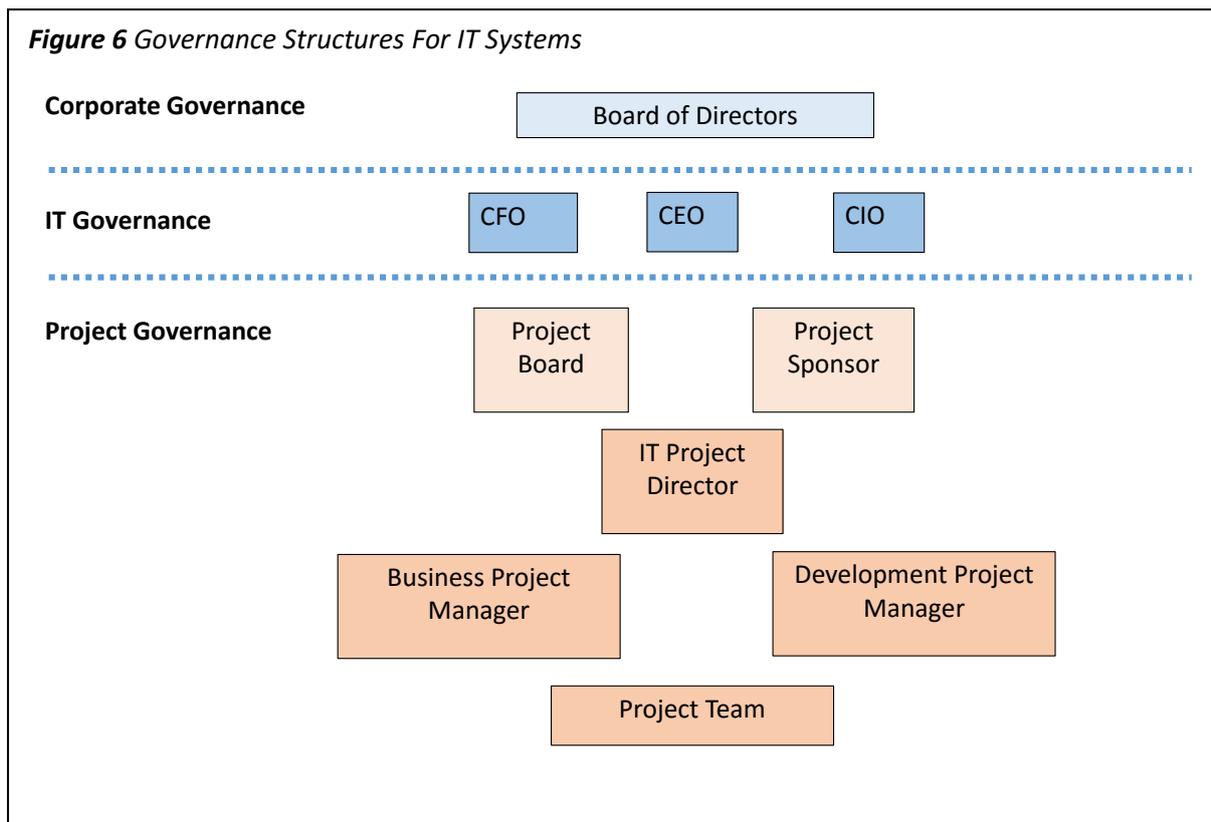
IT systems carry high strategic impact for individuals, organisations, and networks. As a result organisations should manage the IT systems with a great deal of care. Most large organisations formalise their governance systems and have a Chief Information Officer (CIO) that either is a Board Member or reports directly to the board (see figure 6).

⁵⁴ Association of Project Management 2016 "Introduction to Governance" <https://www.apm.org.uk/body-of-knowledge/context/governance/> n

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

Standards are valuable tools for managing conformance and performance. Standards can provide an effective framework for the governance of IT systems and infrastructure. Perhaps, the most widely recognised standard is the COBIT framework (Control Objectives for Information and related Technology). COBIT is an open standard for control over and governance of IT systems developed and promoted by the IT Governance Institute. It is published by the Information Systems Audit and Control Association (ISACA).⁵⁵ The latest iteration of COBIT (COBIT 5) is flexible enough to oversee the incorporation of MDL systems within individual enterprises.

Standards enhance trust in governance structures by enabling third party verification of systems and software. They are also a useful governance tool for applying network wide protocols. System security will be a significant concern for MDL users conducting high volume or high value transactions. Whilst the underlying technology and encryption systems supporting MDLs is extremely robust, the malfeasance of disgruntled employees or the loss or theft of individual keys may leave a network vulnerable to attack. The effective governance of security will enhance trust in MDL networks and in the case of private or consortium MDLs conformance to appropriate security standards can be enforced through SLAs.



⁵⁵ COBIT 5 "Getting Started with COBIT 5" <https://cobitonline.isaca.org/getting-started>

Part 3 Tools And Techniques For The Governance Of MDLs

3.1 The Foundations Of Good Governance

Governance requires 6 elements that form the foundations for effective delivery⁵⁶ (see table 4 and Figure 7). The first five are applicable to all MDL networks, while the last one is primarily of concern to state-sponsored and private/consortium MDL networks.⁵⁷

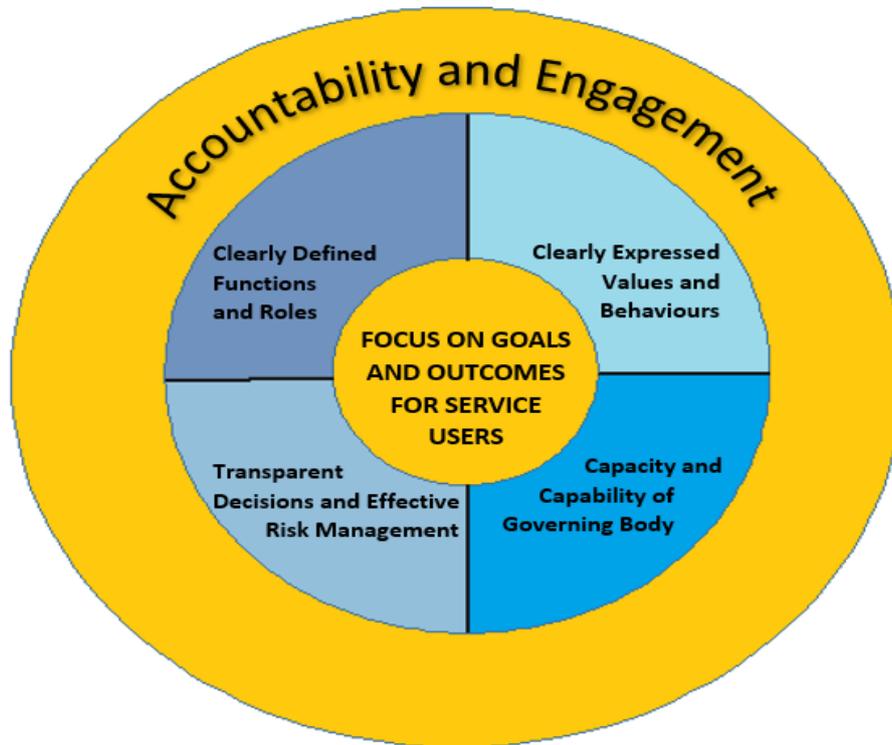
Table 4 *The Foundations of Good Governance For MDLs*

Element	Type of MDL
1. Clarity about the organisation’s purpose and its intended outcomes for stakeholders and service users.	State/Public/Private
2. Clarity about the functions and structure of the governing body.	State/Public/Private
3. Informed, transparent decision-making and managing risk effectively using good quality information, advice, and support.	State/Public/Private
4. Effective stakeholder engagement and accountability.	State/Public/Private
5. Promoting values for the whole network and demonstrating the values of good governance through effective enforcement.	State/Public/Private
6. Developing the capacity and capability of the governing body to be effective by ensuring that board members have the skills, knowledge, and experience they need to perform.	State/Private

⁵⁶ NHS Providers 2015 “*The foundations of Good governance- A compendium of good practice*”
<https://www.nhsproviders.org/media/1738/foundations-of-good-governance-web-file.pdf>

⁵⁷ ICGPS 2004 “*The Good Governance Standard for Public Services*”
http://www.cipfa.org/~media/files/publications/reports/governance_standard.pdf

Figure 7 The Six Core Principles Of Good Governance



3.2 Tools For Effective Governance

MDL networks can use a number of basic tools to deliver effective, transparent, and accountable governance:

Strategic plans should be used to set priorities, focus energy and resources. They should ensure that stakeholders are working toward common goals through establishment of agreements for intended outcomes/results, and through assessment and adjustment of the direction of networks in response to a changing environment.⁵⁸

The objective of strategic planning should be the generation of value for stakeholders⁵⁹ (see figure 8). Value of MDLs is created by increasing the size of the network, removing central intermediaries, simplifying connections between counterparties and recording data on a tamper-proof chain. These measures should improve the speed, and efficiency with which payments are made.⁶⁰

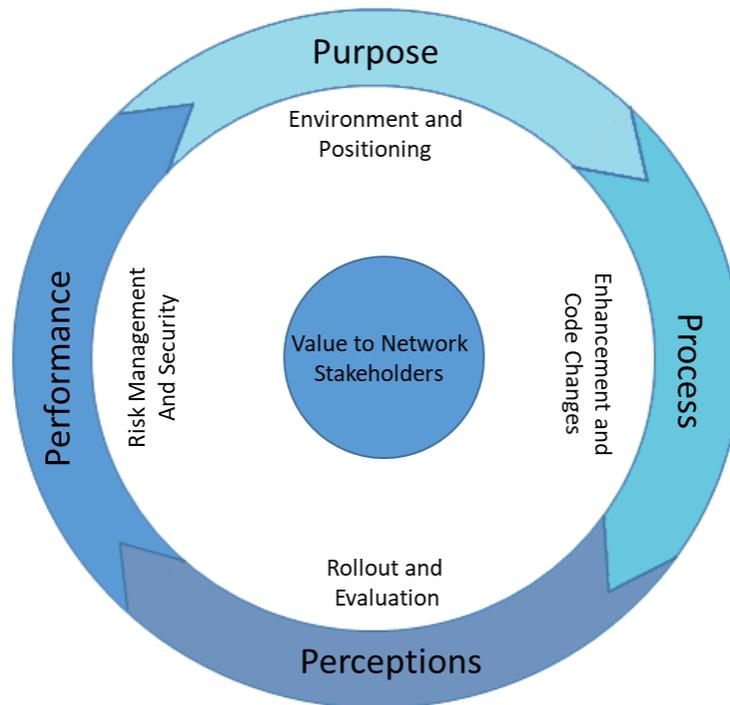
⁵⁸ Kaplan R, Norton S 1996 *"The Balance Scorecard"* Harvard Business School Press ISBN 0-87584-651-3

⁵⁹ Whittmann R and Reuter M 2009 *"Strategic Planning How to Deliver Maximum Value Through Effective Business Strategy"* Kogan Page ISBN-10: 0749452331

⁶⁰ Williams et al 2016 *"Distributed Ledgers in Payments: Beyond the Bitcoin Hype"*

<http://www.bain.com/publications/articles/distributed-ledgers-in-payments-beyond-bitcoin-hype.aspx>

Figure 8 Enhancing Value For MDL Stakeholders Through Effective Strategy



In addressing strategy development for MDLs, the following issues should be considered:

1. **Perceptions** by Stakeholders can be managed through effective consultation. There are four stakeholder groups that should be taken into account: users, the public, regulators, and developers.
2. **Performance** relates to the following questions:
 - What goals and timelines have been set for the MDL? Are these being delivered efficiently and effectively?
 - What performance agreements have been established and are these being met?
3. **Purpose** focuses on the operational goals for the MDL. One critical question is whether the operating environment has changed, and if it has what new opportunities and threats have emerged.
4. **Process** analysis can help identify inefficiencies and recommend potential for enhanced productivity of the network.

Performance management frameworks should detail progress against the goals and targets specified in the strategy. The framework should identify performance benchmarks and ensure that performance improves over time. Performance management standards have

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

yet to be developed for MDLs⁶¹ but a range of standardised business tools, such as the ‘balanced scorecard’ approach, could be adapted for private networks (see Project Governance for MDLs) and enforced through service level agreements.

Auditing and reporting arrangements are fundamental to enforce accountability and promote trust in governance arrangements.⁶² The financial services sector, and by extension the MDL systems used within it, are subject to extensive regulations supported by penalties for non-conformance.

Users of MDLs may chose third party audits or conformity assessments, such as those used in the voluntary standards market, to reduce the risk of non-compliance. Voluntary standards markets are commercial systems in which actual and potential buyers and suppliers of products and services rely on conformity assessments carried out against standards. These assessments may comprise first, second or third-party verification and certification. Voluntary standards markets are used widely in all industries and bridge regulated and unregulated markets.⁶³

MDLs can be built in a wide variety of ways for a wide variety of purposes. A crypto-currency ledger supports a proof-of-work consensus mechanism. An internet-of-things data logging MDL is designed for speed and efficiency. Both may be subject to audit: not just for crypto-currency cash tracking, but also for, say, billing or liabilities.

Although the technology supporting MDLs is not especially complicated, these ‘multi-organisational databases with a super audit trail’ are built on foundations which may be unfamiliar to many, even programmers using them.⁶⁴ Cryptography and hashing are two core techniques for MDLs. Cryptography is the process of storing data in such a way that it can only be read by those with the correct keys. Hashing is the process of reducing computer files to an individual, unique signature. MDLs are constructed by hashing records along with previous hashes to form a chain, but often use other cryptographic techniques as well.

If the MDL is not just recording, but supporting a token or crypto-currency, then a host of transaction validation techniques may need to be understood, such as proof-of-work, proof-of-stake, proof-of-burn, full consensus, broadcasting, or voting mechanisms.

If the MDL is a smart ledger, then many of the rules are based in pieces of code embedded within the MDL itself.

⁶¹ Mainelli M & Mills S 2016 “*The Missing Links In The Chains? Mutual Distributed Ledger (aka blockchain) Standards*”

[http://www.zyen.com/PDF/The_Missing_Links_In_The_Chain_Mutual_Distributed_Ledger_\(aka_blockchain\)_Standards_2016.11_v2.4.pdf](http://www.zyen.com/PDF/The_Missing_Links_In_The_Chain_Mutual_Distributed_Ledger_(aka_blockchain)_Standards_2016.11_v2.4.pdf)

⁶² ICAEW 2006 “*Audit Fundamentals - Audit purpose*”

⁶³ Mainelli M and von Gunten C 2013 “*Backing Market Forces: How To Make Voluntary Standards Markets Work For Financial Services Regulation*” BSI, Chartered Institute for Securities & Investment and Long Finance

⁶⁴ Mainelli M “*Blockchain – dark currencies and the risks*” ACCA

<http://accaibulletin.newsweaver.co.uk/accaiabulletin/3khryf0dpp07latets9jci?email=true&a=1&p=51679230&t=28194286>

Responsibility Without Power?

The Governance Of Mutual Distributed Ledgers

Defining the boundary of the system is challenging, as it encompasses not just a crypto-currency, but also the wallets and exchanges that are used for the transactions. The MDL is itself subject to attacks. Crypto-currencies are seen by many as big 'honeypots', worth probing and attacking by hackers because the rewards for stealing crypto-currency can be enormous. An auditor examining a crypto-currency system would need to trace accounts from their ledger into other crypto-currencies that had been used for payment. The auditor must:

- ◆ Trace the sources of funds from wallets and exchanges that had made the deposits.
- ◆ Identify where transactions had potential conflicts with regulatory jurisdictions.

Although MDLs are likely to reduce the role of trusted third parties (central authorities) and diminish the need for safeguarding, central third parties will still be needed to:

1. Confirm the existence of the asset to be traded, be it money, securities, or other assets.
2. Verify community membership.
3. Ensure compliance with law and regulators.
4. Guarantee the rights of those participating in the transaction.

Risk management plans should analyse the likelihood of adverse events occurring, the impact on the MDL and the strategies to mitigate and manage these risks.⁶⁵ Significant risks should include changes in the business or regulatory environment, their impact on the MDL and the stakeholders.

A wide range of tools is available to organisations that seek to manage risk effectively. ISO 31000 offers an effective and flexible approach that is suitable for use with MDLs. A list of potential risks for MDL networks is listed in Table 5.

⁶⁵ Hopkins P 2017 "*Fundamentals of Risk Management*" (fourth edition) Kogan Page ISBN-13: 978-0749479619

Responsibility Without Power?
The Governance Of Mutual Distributed Ledgers

Table 5 Potential Risks for MDL Networks

Risk	Description
Exception Management Failure	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. This may require the need for trusted third parties, which would potentially negate one of the principal selling points of MDLs. Failure to deal with exceptions effectively could lead to litigation and loss of trust in the MDL network.
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. Indemnity and insurance arising on smart ledgers should be considered in the event that a digitally signed document proves to be fraudulent.
Anonymity and Reputation	Criminal use of MDLs may prompt a legislative repose by government(s) lifting the anonymity of MDL users.
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 make compliance complex. Action should be taken to ensure that users of an MDL network are not jointly and severally liable for breaches.
Security	Malicious access to a private MDL, for example using a stolen key, would 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. Effective systems should not only reduce the risk of this happening, but they should also identify procedures to take swift and effective action to repair damage, seal the breach, and ensure network stability.
Transparency & Reporting	Data encryption in MDLs could further complicate risk management and oversight, particularly in securities. MDLs should be designed to facilitate third party audit.
Performance	New technology developments may prompt network users to migrate to MDLs with higher transaction speeds. Strategic and risk management plans should identify these risks and take steps to respond to them.

CONCLUSION

MDL technology is in an emergent phase. New applications are under development. New uses are being researched. New consortia are being formed to explore MDL applications.

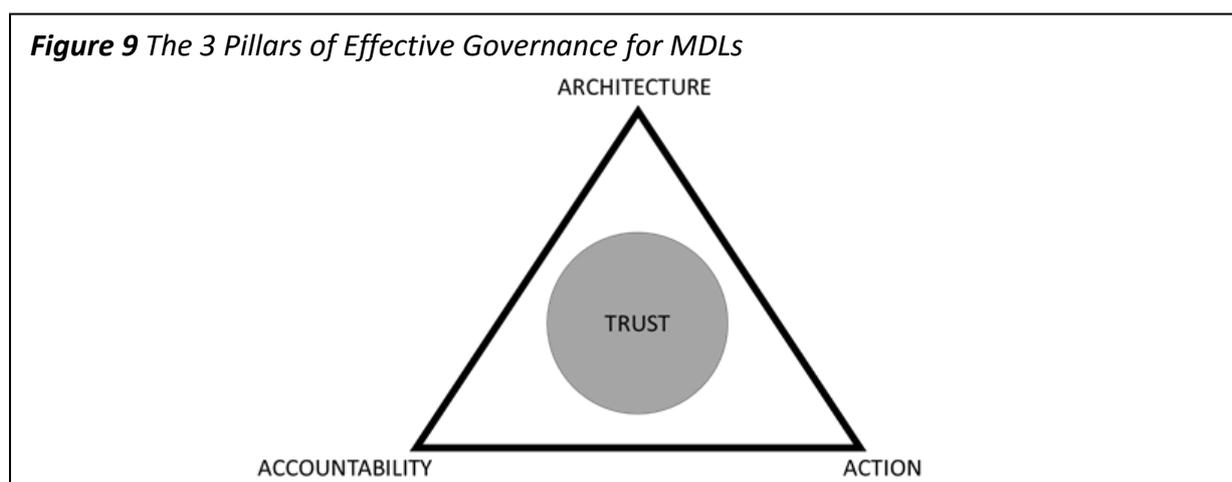
During the course of this research the emergence of Initial Coin Offerings (ICO) was mentioned by several of the individuals we consulted. ICO “coins” are essentially digital coupons, tokens issued on an MDL, or blockchain, of the kind that underpins cryptocurrencies. Investors hope that successful projects will cause tokens’ value to rise⁶⁶.

Consideration of appropriate governance structures for ICOs and other types of MDL have, until now, been given a lower priority than technical issues, although tools to assist MDLs with developing appropriate governance structures are beginning to emerge.⁶⁷

Ultimately, effective governance in MDL systems relies on people rather than software, and rests on three pillars:

1. **Architecture:** The role of the governance structure, its composition, remit, powers, responsibilities, and its relationship with users, is a critical component.
2. **Accountability:** Effective governance of MDLs enhances trust. Trust is enhanced when a governance structure is accountable to its stakeholders, transparent in its decision-making, and subject to periodic audit and third party review.
3. **Action:** The governance structure must develop strategic and risk management plans, which are delivered through effective performance management frameworks. Trust can be further enhanced through the use of the voluntary standards market to independently verify performance metrics and the systems established to compile them.

Table 7 presents a simple checklist highlighting the key issues that organisations should consider in creating a strong and stable foundation for these three pillars.



⁶⁶ Economist 2017 “The market in Initial Coin Offerings risks becoming a bubble”
<https://www.economist.com/news/finance-and-economics/21721425-it-may-also-spawn-valuable-innovations-market-initial-coin-offerings>

⁶⁷ WEF 2017 “Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies” World Economic Forum White Paper June 2017

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

Table 6 Simple Checklist of Governance Issues for MDL Networks

	Public MDL	State-Sponsored MDL	Private MDL	Consortium MDL
Architecture	What is the legal framework for the MDL?	Which department owns the MDL?	What is the legal framework for the MDL?	What is the legal framework for the MDL?
	How is consensus created?	How is policy made and rolled out?	How is policy developed and rolled out?	How are consortium members represented?
	How are decisions made, particularly with respect to changing rules or software?	How does MDL policy fit within the wider policy environment?	How are decisions made, particularly with respect to changing rules or software?	How are decisions made, particularly with respect to changing rules or software?
	How are decisions enforced?	Does the oversight committee have sufficient technical expertise?	How are decisions rolled out?	How are decisions enforced?
	Does the network have paid employees? Who manages them?	Who does the oversight committee report to?	Does the board have sufficient expertise in both the technology and the sector where it is being applied to?	Does the oversight committee have sufficient technical expertise?
	How are user disputes resolved?	What mechanism has been established to deal with complaints?	How are user disputes resolved?	How are disputes between consortium members resolved?
	Is there a clear separation of the functions of power?	Is the legislative branch sufficiently engaged?	Has a service level agreement been developed?	Does the consortium have paid employees? Who manages them?
	Does the parent structure have a written constitution which details terms of use as well as governance?	Does the legislative branch have sufficient technical expertise to understand the implications of policy changes to the MDL?	How is delivery of the SLA monitored and what are the penalties for variance?	Does the consortium have a foundation agreement which lays out terms of service?
Accountability	Who are the stakeholders?			
	How are stakeholders concerns represented?			
	Is there a central record of decision making?			
	Is there a mechanism for stakeholders to challenge decisions?			
	Are there independent mechanisms for resolving disputes by mediation, arbitration or expert determination? How are these mechanisms enforced?			
Action	Has a strategic plan been developed?			
	Has a Risk Management Plan been developed?			
	Has a Performance Management framework been created?			

Responsibility Without Power?
The Governance Of Mutual Distributed Ledgers

	What arrangements have been made for reporting, third party audit, and verification? How will stakeholder access these reports?	What arrangements have been made for reporting and auditing? Who will have access to these reports?	What arrangements have been made for reporting, third party audit, and verification? Will users have access to these reports?	What arrangements have been made for reporting, third party audit, and verification? How will consortium members have access to these reports?
--	---	---	---	--

Glossary

Board	the structure responsible for governance of the MDL.
Consortium	an association of two or more organizations or governments (or any combination of these entities) with the objective of participating in a common activity or pooling their resources for achieving a common goal.
Crypto-currency	a currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.
Enterprise	a business, academic institution, government department or non-governmental organisation.
GDPR	General Data Protection Regulations are a data protection regime introduced by the EU in 2016 for application from 2018 with heightened requirements on organisations to implement measures to protect sensitive data, and giving citizens the 'right to be forgotten'.
ICO	an Initial Coin Offering is a fundraising tool that trades future cryptocurrencies in exchange for crypto-currencies of immediate, liquid value. Initially established to launch new types of

Responsibility Without Power? The Governance Of Mutual Distributed Ledgers

	crypto-currency, ICOs are now used a crowdfunding tools for a wide variety of projects.
Mining	the process of adding transaction records to Bitcoin's public ledger of past transactions, with new bitcoin as a reward
Node	a dedicated server which stores and rebroadcasts validated blocks and transaction across an MDL network.
Organisation	an entity with a particular purpose, such as the establishment and maintenance of an MDL.
Ricardian Contract	a digital contract, which contains all terms and clauses of a legally conventional written contract but it is readable both by people and by software.
Smart contract	a contract clause translated into computer code through a rigorous process and embedded in a database or MDL, which executes automatically when its trigger conditions are met.
Stakeholder	an individual or organisation which is affected by the data held on the MDL.
User	an individual or organisation with permission to add data to, or access information held on, the MDL.



“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:

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

www.longfinance.net

A Report Prepared By The Z/Yen Group
Principal authors: Simon Mills & Bob McDowall
© Z/Yen Group Limited, July 2017



Z/Yen Group Limited

41 Lothbury, London EC2R 7HG, United Kingdom

+44 (0) 20 7562-9562 (telephone)

hub@zyen.com (email)

www.zyen.com

SPONSORED BY



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