The Journal of Financial Perspectives: FinTech

Article:

Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)

EY Global Financial Services Institute **Winter 2015 | Volume 3 – Issue 3**

Professors Michael Mainelli and Mike Smith
Z/Yen Group Limited

Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)

Michael Mainelli
Executive Chairman, Z/Yen Group Limited[1]

Mike Smith
Associate Director – Systems Architecture, Z/Yen Group Limited

[1] We owe special thanks to Mary O'Callaghan, Project Manager of the InterChainZ project, and the other team members, Ben Morris, Xueyi Jiang, Chiara von Gunten and Mark Duff of Z/Yen. Our very special thanks go to Suncorp, PwC and DueDil that not only funded the research, but were also active collaborators. We were pleased to have the active involvement of a regulatory jurisdiction in Alderney. We benefited enormously from delightful interaction with Ethereum

Abstract

Mutual distributed ledgers (MDLs) have the potential to transform the way people and organizations handle identity, transaction and debt information. MDL technology provides an electronic public transaction record of integrity without central ownership. The ability to have a globally available, verifiable and untamperable source of data provides anyone wishing to provide trusted third party services, i.e., most financial services firms, the ability to do so cheaply and robustly. Blockchain technology is a form of MDL.

The InterChainZ project was a consortium research project to share learning on MDLs during the summer of 2015. The study found that InterChainZ showcased several distributed ledger configurations and numerous variants, exploring how they might work in a set of agreed "use cases." The outputs were a series of functioning, interlinked MDLs along with software, explanatory materials and website information. The research consortium concluded that MDLs incorporating trusted third parties for some functions had significant potential in financial services, such as know-your-customer (KYC), anti-money-laundering (AML), insurance, credit and wholesale financial services.

"Although the monetary aspects of digital currencies have attracted considerable attention, the distributed ledger underlying their payment systems is a significant innovation." ... "the potential impact of the distributed ledger may be much broader than on payment systems alone. The majority of financial assets – such as loans, bonds, stocks and derivatives – now exist only in electronic form, meaning that the financial system itself is already simply a set of digital records." Bank of England, Quarterly Bulletin (2014, Q3)

1. Background

1.1 What is trust in financial services?

Trust leverages a history of relationships to extend credit and benefit-of-the-doubt to someone. Trust is about much more than just money; it is about human relationships, obligations, experiences and about anticipating what other people will do. In risky environments trust enables cooperation and permits voluntary participation in mutually beneficial transactions that are otherwise costly to enforce, especially by third parties. By taking a risk on trust, we increase the amount of cooperation throughout the society while simultaneously reducing the costs, unless we are wronged. Trust is not a simple concept, nor is it necessarily an unmitigated good, but trust is the stock-in-trade of financial services. In reality, financial services trade on mistrust. If people trusted each other on transactions, many financial services might be redundant.

Technology is transforming trust. There are reputational ranking systems from point scores on Amazon, to supplier ratings on eBay, to collaborative filtering on many sites, to "I hate" websites, to social networks with referral or testimonial systems. We have fictional reputational currencies, such as the Whuffie, being realized in novel real ones such as Ripple with its Trust Lines. As a means of transacting business over space, never before has there been a time when it has been easier to start a distant geographic relationship. With a credible website and reasonable links, people are prepared to learn about companies half a world away and entertain the idea of conducting commerce with them. Society is changing radically when people find themselves trusting first encounters people with whom they have had no experience, e.g., on eBay or Facebook, less experience than on a first encounter with a local corner store.

Box 1: Ship registry skit

The ship registry skit – part 1: validating
Shady Shipper: "I'd like to register my vessel. Here's a photo I took on the island this morning of my supertanker berthed at the port terminal." Scrupulous Registrar: "We need a bit more than that to go on, your purchase certificate, IMO ship registration number, tonnage certificate, load line certificate …" Shady Shipper: "Here's U.S.$10,000." Scrupulous Registrar: "That will do nicely, Sir."

The ship registry skit – part 2: transacting
Shady Shipper: "I'd like to sell my vessel once to Otto and once to Maria." Sanctimonious Registrar: "But that's not possible." Shady Shipper: "Here's U.S.$10,000." Sanctimonious Registrar: "That will do nicely, Sir."

The ship registry skit – part 3: recording
Shady Shipper: "I have to go court and need you to change your historical records for me such that only Maria is shown to own the ship." Shady Registrar: "That could cost you…" Shady Shipper: "Here's U.S.$10,000." Shady Registrar: "That will do nicely, Sir."

People use trusted third parties in many roles in finance, as custodians, as payment providers, as poolers of risk, i.e., insurers. The "ship registry" skit in Box 1 illustrates three core functions that trusted third parties perform:

- **Validating:** identifying the existence of something to be traded and membership of the trading community
- **Transacting:** preventing duplicate transactions, i.e., someone selling the same thing twice or "double spending"
- **Recording:** holding the record of transactions in the event of dispute

If faith in the technology's integrity continues to grow, then MDLs might substitute for two roles of a trusted third party, preventing duplicate transactions and providing a verifiable public record of all transactions. Trust moves from the third party to the technology.

Emerging techniques, such as smart contracts and decentralized autonomous organizations, might in future also permit MDLs to act as automated agents. The consequence may be that the first role of a trusted third party, authenticating an asset and identifying community members, becomes the most important.

1.2 What is a ledger?

A ledger is a book, file or other record of financial transactions. People have used various technologies for ledgers over the centuries. The Sumerians used clay cuneiform tablets for recording transactions. Medieval folks used split tally sticks. So much so that in England, when tally sticks were retired in 1834, the destruction of tallies got so out of control that they burned down the Houses of Parliament. In the modern era, the implementation of choice for a ledger is a database, found in all modern accounting systems.

When many parties interact and need to keep track of complex sets of transactions they have traditionally found that creating a centralized ledger is helpful. A centralized transaction ledger needs a trusted third party who makes the entries (validates), prevents double counting or double spending (safeguards) and holds the transaction histories (preserves). Over the ages, centralized ledgers are found in registries (land, shipping, tax), exchanges (stocks, bonds) or libraries (index and borrowing records), just to give a few examples. But while a third party may be trusted, it does not mean they are trustworthy.

The implementation of choice for a centralized ledger is a centralized database run by a trusted third party, such as a bank, an insurer, an exchange or a registry. Robert Sams describes a centralized transaction ledger's three weak points as "sin of commission" – forgery of a transaction; "sin of deletion" – reversal of a transaction; and "sin of omission" – censorship of a transaction. These weak points correspond to the three roles of a trusted third party – validation, safeguarding and preservation.

1.3 What is an MDL?

A distributed ledger is a technology that securely stores transaction records in multiple locations. The implementation of choice for a distributed ledger is a distributed database. "Distributed database: 1. A database that is not entirely stored at a single physical location, but rather is dispersed over a network of interconnected computers.

2. A database that is under the control of a central database management system in which storage devices are not all attached to a common processor." – Federal Standard 1037: Telecom Glossary (7 August 1996) – http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm

MDLs allow groups of people to validate, record and track transactions across a network of decentralized computer systems with varying degrees of control of the ledger. Everyone shares the ledger. The ledger itself is a distributed data structure held in part or in its entirety by each participating computer system. The computer systems follow a common protocol to add new transactions. The protocol is distributed using peer-to-peer application architecture. In short, an MDL is a secure peer-to-peer ledger with storage analogous to peer-to-peer file sharing systems such as Gnutella, "Gnutella for accountants."

Peers are equally privileged participants in the protocol. MDLs are not new – concurrent and distributed databases have been a research area since at least the 1970s. Historically, the primary purpose of a distributed database was the continued existence of a ledger in multiple locations in extreme circumstances, for example during warfare. Distributed databases were persistent and pervasive. Defense organizations used distributed databases for this reason in the 1970s. A slightly more complicated distributed database approach allows people to continue to record new transactions in multiple locations with only periodic communication. Distributed databases of this form have been used for remote mutual working, allowing people to share information yet preventing errors arising in the ledger, or forms of mutual long-term archiving and backup.

Historically, distributed ledgers have suffered from two perceived disadvantages: insecurity and complexity. These two perceptions are changing rapidly due to the growing use of blockchains, a form of distributed database that has found success as the distributed ledger of choice for cryptocurrencies.

2. What is a blockchain?

Nick Williamson believes "that a blockchain consists of three main, complementary parts: a shared state, a set of rules for updating state via blocks and a trust model for timestamping." [Williamson (2015a)]

Williamson's three complementary parts correspond well with the trusted third-party ledger model introduced above: validate – a trust model for timestamping new transactions by members of the community; safeguard – a set of rules for sharing data of guaranteed accuracy; and preserve – a shared view of the history of transactions.

In January 2009, blockchain technology was used to help create Bitcoin, a cryptocurrency-based protocol for the exchange of tokens called bitcoins. Bitcoin and other cryptocurrencies (also called AltCoins) gained significant attention in 2013 with Bitcoin's sharp price rise when transacted in fiat currencies, the historic high being U.S.$1,124.76 on 29 November 2013. Bitcoin market capitalization dropped from a high of U.S.$13.9 billion on 4 December 2013 to about U.S.$3.3 billion in May 2015. High prices and high volatility attracted speculation, as well as proliferation of competitive and complementary cryptocurrencies. Arguably, there are over 600 AltCoins based on blockchain technology. Bitcoin remains the preponderant cryptocurrency. The market capitalization of the top 600 cryptocurrencies tracked by http://coinmarketcap.com/all/views/all/ including Bitcoin is U.S.$3.9 billion. Technologists have drawn attention to the MDL underpinning cryptocurrencies, the blockchain.

A blockchain is a transaction database based on a mutual distributed cryptographic ledger shared amongst all nodes participating in a system. It is public in that it is decentralized and shared by all nodes of a system or network. There is integrity as double spending is prevented through block validation. The blockchain does not require a central authority or trusted third party to coordinate interactions, validate transactions or oversee behavior. A full copy of the blockchain contains every transaction ever executed, making information on the value belonging to every active address (account) accessible at any point in history.

The blockchain's main innovation is a public transaction record of integrity without central authority. The blockchain is decentralized by nature, i.e., shared by all nodes connected to a set network. Blockchain technology offers everyone the opportunity to participate in secure contracts over time, but without being able to avoid a record of what was agreed at that time

While Bitcoin is problematic legally, socially and economically, and there have been technical glitches with Bitcoin wallets, the blockchain technology has proven robust. In fact, as an experiment in proving blockchain technology's robustness, Bitcoin has been superb, showing the technology to be proof against a wide range of attacks, from criminals to national security agencies. Growing confidence has led numerous firms, particularly in financial services, to announce their interest in using them: Nasdaq, BNY Mellon, UBS, USAA, IBM, Samsung and many others. In turn, a number of firms have realized that the wider field of MDLs provides a variety of approaches that can be adapted to numerous uses.

2.1 Why is the Bitcoin blockchain important?

The Bitcoin blockchain is important because it showed that distributed ledgers could work in harsh environments of little, no, or even negative, trust. The Bitcoin blockchain has been challenged by businesses, criminals, law and security agencies. So far, though there have been some hiccups, the blockchain has not been compromised. Further, while more complex than a centralized ledger, the complexity of the blockchain is comprehensible and provides commensurate benefits for multi-party transactions. This change of perception, from distributed ledgers being "too insecure and too complex" to "it's the blockchain, stupid," has led people to reconsider the use of other types of MDLs in other applications.

For those interested in seeing some older, related MDL applications similar to blockchain thinking, the bullet points below provide a quick sampler (note: Z/Yen itself implemented a semi-distributed encrypted ledger in 1996 in the U.K. for a sensitive case management system):

- 1993 – "Encrypted open books" – 1993 – "Encrypted open books" – https://www.marc.info/?l=cypherpunks&m=85281390301301&w=3
- 1995 – "WebDNA" – http://www.webdna.us/page.dna?numero=27 & http://en.wikipedia.org/wiki/WebDNA
- 1996 – "Ricardo payment system" – http://www.systemics.com/docs/ricardo/execsummary.html

- 1999 – Stanford University's CLOCKSS (Controlled lots of copies keep stuff safe) http://www.clockss.org/clockss/Home and LOCKSS (Lots of copies keep stuff safe) – http://www.lockss.org/about/history/ for archiving
- 2004 – Ripple, a consensus ledger approach to currency transactions – https://ripple.com/

While a work of significant technical ingenuity, the Bitcoin blockchain could be equally regarded as just a new assemblage of existing components. The principal components are public-key cryptography (Diffie–Hellman circa 1976) and a proper decentralized peer-to-peer network (Gnutella 2000). The use of these technologies in Bitcoin "mining" was ground-breaking, by applying an approach to Byzantine Fault Tolerance to the problem of transaction verification, though even here there was some precedent in a short 1998 paper on b-money by Wei Dai. The two technical weaknesses are also apparent.
If public-key cryptography is cracked, or internet peer-to-peer somehow switches off, then cryptocurrencies would fail, along with much else in modern finance starting with credit cards.

Although cryptocurrencies have proven one form of MDL, blockchains, in a very harsh environment, once one relaxes some of the conditions, e.g., give back a trusted third party some of their role, a huge range of possible approaches that have been around a while open up. MDL technology promotes speculation. What if any group of companies could elect to create their own pooling system on the spot? What if a group of shippers decided to establish a shared carriage system for containers? What if a property developer elected to mandate participation among all their suppliers? Each supplier might buy all materials and goods such as cement or cabling from a central store under a sophisticated averaged pricing algorithm incentivizing each to buy cheaply and share fairly. We can easily imagine instant mini-insurers creating a shared economy approach to special purpose vehicles.

By relaxing conditions, e.g., assuming a trusted third party might perform some validation role, there are opportunities to throw away the expensive "mining" and keep the ledger. Before getting too carried away that all financial services will move to variants of the blockchain, it is worth quoting some informed skepticism (Box 2).

Box 2: Skepticism toward blockchain

"...we have reflected tiny bursts of enthusiasm for what blockchain technology, the distributed public ledger underpinning bitcoin, could do for the murky and shadowy world of OTC bilateral clearing.

Such enthusiasm should not, however, be confused with the current industry vogue of rubbishing bitcoin while simultaneously claiming that the blockchain technology is genius.

We are less sanguine on the latter front.

For one, we're not convinced blockchain can ever be successfully delinked from a coupon or token pay-off component without compromising the security of the system. Second, we're not convinced the economics of blockchain work out for anything but a few high-intensity use cases. Third, blockchain is always going to be more expensive than a central clearer because a multiple of agents have to do the processing job rather than just one, which makes it a premium clearing service — especially if delinked from an equity coupon — not a cheaper one."

Kaminska, I., 2015, "On the potential of closed system blockchains," FT Alphaville, 19 March - http://ftalphaville.ft.com/2015/03/19/2122148/on-the-potential-of-closed-system-blockchains/

FinTech, a combination of "financial" and "technical" or "technology," refers to the proliferation of new applications delivering financial services directly to devices. FinTech applications all need ledgers, and it is easy to conclude that there will be a proliferation of MDLs as well. FinTech devices frequently spawn currency or point schemes, such as air mile or supermarket point schemes. Ledgers also track "chain of custody" of assets. For example, shipping companies could use an MDL for all sorts of documentation tracking, bills of lading, letters of credit, load line exemptions, etc. The payment information, which might be going through SWIFT transactions, would be recorded in an MDL when it was relevant. SWIFT stays as it is, but the shipping industry gets new services. There are "chain of custody" situations in forestry, pharma, wine or fish, to take a few examples, where similar approaches could be used — and people are starting to do it (blood diamonds http://blocktrace.io/, or more general social and ethical tracing https://www.provenance.org/).

The list of possible applications in financial services is growing rapidly. Figure 1 (overleaf) summarizes just some of the more outstanding ones.

People use trusted third parties in many roles in finance, as custodians, as payment providers, as poolers of risk, i.e., insurers. As mentioned earlier, trusted third parties in finance provide three functions: validation, safeguarding and preservation. If one believes in the integrity of distributed ledgers, then they might largely displace two roles of a trusted third party, no double spending and providing a verifiable public record of all transactions. Such displacement might also increase the importance of the first role, validating the existence or community membership of something in the first instance. Moreover, increased confidence in technology performing two third-party functions — safeguarding and preservation — should lower the barriers and costs of setting up trusted third-party services, and perhaps lead to increased demand.

Personal identity verification, authentication and data management could bring significant benefits for many sectors. In insurance, the streamlining of digital authentication and better management of personal data and history disclosure could translate into more direct and efficient relationships between insurance companies and individuals. Over time, this could bring additional benefits by reducing identity and claim frauds. In KYC and AML processes, an identity distributed ledger application could transform service levels.

Figure 1: Possible applications of blockchain in financial services

Area	Possible applications
Financial instruments, records, models	Currency, private and public equities, certificates of deposit, bonds, derivatives, insurance policies, voting rights associated with financial instruments, commodities, derivatives, trading records, credit data, collateral management, client money segregation, mortgage or loan records, crowdfunding, P2P lending, microfinance, (micro)charity donations, account portability, airmiles and corporate tokens, etc.
Public records	Land and property titles, vehicle registries, shipping registries, satellite registries, business license, business ownership/incorporation/dissolution records, regulatory records, criminal records, passport, birth/death certificates, voting ID, health and safety inspections, tax returns, building and other types of permits, court records, government/listed companies/civil society, accounts and annual reports, etc.
Private records	Contracts, ID, signature, will, trust, escrow, any other type of classifiable personal data (e.g., physical details, date of birth, taste) etc.
Semiprivate/ semipublic records	High school/university degrees and professional qualifications, grades, certifications, human resources records, medical records, accounting records, business transaction records, locational data, delivery records, genome and DNA, arbitration, genealogy trees, etc.
Physical access	Digital keys to home, hotel, office, car, locker, deposit box, mail box, Internet of Things, etc.
Intellectual property	Copyrights, licenses, patents, digital rights management of music, rights management of intellectual property such as patents or trademarks, proof of authenticity or authorship, etc.
Other records	Cultural and historical events, documentaries (e.g., video, photos, audio), (big) data (weather, temperatures, traffic), SIM cards, archives, etc.

Finally, perhaps we should coin "RegTech," a proliferation of new applications regulating financial services directly on devices. RegTech would need to cover everything from systems that monitor and control core ledgers to the "purses" on the periphery that store value locally with users. Regulators could insist on people recording transactions externally on MDLs, thus reducing the cost of firm failures, providing open sources of transaction prices and volumes, or increasing competition through increased data portability, e.g., switching financial accounts.

2.2 MDL architectures

MDLs can be implemented in a number of ways. Changing the type of ledger or relaxing some constraints releases a huge range of possibilities. For example, by reintroducing trusted third parties or regulators, one can "throw away the expensive mining" yet keep the ledger.

There are numerous technical choices on cryptography standards, peer-to-peer arrangements, guaranteed distribution approaches, partial cryptography, programming languages, communication protocols, etc. Perhaps the most general implementation choices are: public versus private — is reading the ledger open to all or just to defined members of a limited community?

Permissioned versus permissionless — are only people with permission to add transactions, or can anyone attempt to add a transaction? Proof-of-stake, proof-of-work, consensus or identity mechanisms — how are new transactions authorized? True peer-to-peer or merely decentralized — are all nodes equal and performing the same tasks, or do some nodes have more power and additional tasks?

The Bitcoin blockchain is just one type of public, permissionless, proof-of-work, peer-to-peer distributed ledger. One categorization of leading approaches runs as follows [adapted from Mougayar (2015)]:

1. **Bitcoin currency + Bitcoin blockchain:** Bitcoin. A public, permissionless, proof-of-work, peer-to-peer reference point.
2. **Bitcoin currency + non-Bitcoin blockchain:** Blockstream, Truthcoin. Side chains are "pegged" to the main Bitcoin blockchain via various schemes.
3. **Non-Bitcoin currency + Bitcoin blockchain:** Factom, Mastercoin, Counterparty, Namecoin. In this case, the Bitcoin blockchain is used, but a native currency or token is added.
4. **Non-Bitcoin currency + non-Bitcoin blockchain:** Ethereum, BitShares, Truthcoin, Litecoin, PayCoin. New types of blockchains and new currencies.
5. **Non-blockchain consensus or identity:** Ripple, Stellar, NXT, Hyperledger, Tendermint, Pebble, Open Transactions, Z/Yen's InterChainZ. Decentralized platforms with new types of MDLs.
6. **Blockchain-neutral smart services:** Eris Industries, PeerNova, Codius, SmartContract, SAE, Tezos, Tillit. This category is still developing, but includes a mix of decentralized platforms and dumb/smart contracts.

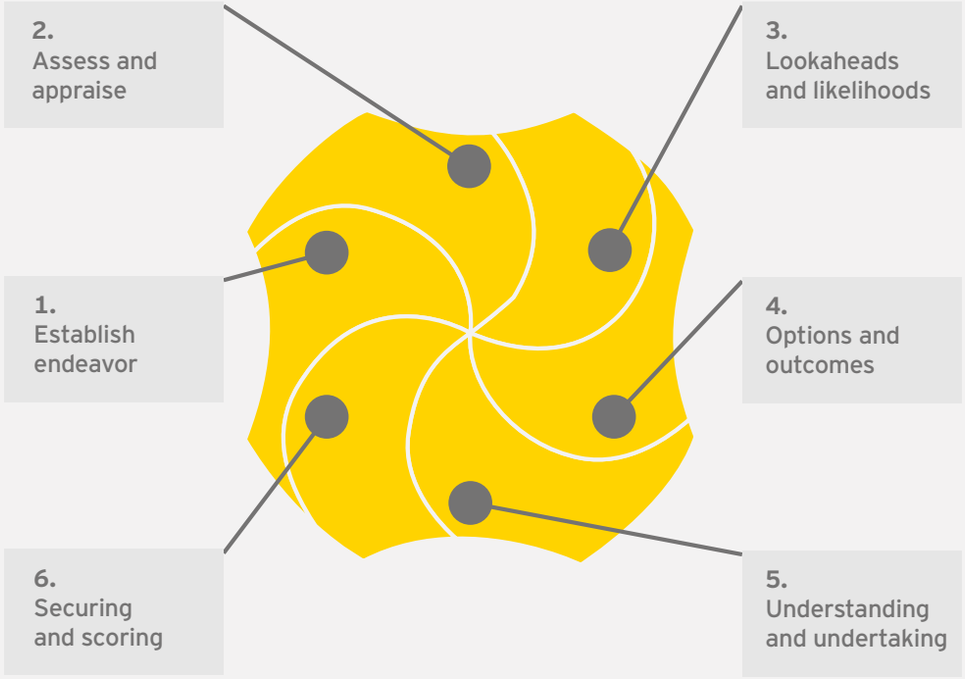
3. InterChainZ

3.1 Project summary

InterChainZ was a cooperative research project aimed at providing a generic demonstration pilot of how MDL technology might provide such capabilities for current financial services.

InterChainZ aimed to answer a core question – "what elements of a trusted third party are displaced by MDL technology?" by providing a basic demonstrator of distributed ledgers, including variants of blockchains, and comparing how they might work within selected financial services use cases. The objective was to build a small suite of software providing an interface to MDLs for tasks such as selection and storage of documents, document encryption, sharing keys, viewing the MDL transactions and viewing the MDL contents subject to encrypted limits.

Figure 2: Z/EALOUS methodology



The software permitted testing a variety of MDL configurations. Suite of software was then used to discuss and test various options for MDLs. The outputs were shared with participants as joint intellectual property for their own future use. InterChainZ provided:

- A demonstrator showing the potential applications in action, specifically: simple ledger for data of any sort, identity application for a person, identity application for a company, personal insurance policy (motor) placement, small business insurance policy placement, arge-scale, long-term storage application or archive and various tests of supervisor nodes and voting validation
- Software available for sharing with consortium members
- A project video, presentation, website and training materials

3.2 Methodology

The research process was divided into six stages, following Z/Yen's Z/EALOUS methodology.

3.2.1 Establish endeavor

In the first stage of research, the consortium members led by Z/Yen Group agreed on the scope, objectives and approach of the research. In particular, it was agreed that the research team would explore several architectures, including Z/Yen's InterChainZ, Ethereum and other variants. The research team started approaching other organizations operating distributed ledger software. The consortium also agreed to contrast and compare selected distributed ledger software on performance, resilience and security by exploring how they worked in the set of four agreed "use cases:"

Global accountancy firm – identity validator: This use case demonstrated the distributed ledger functionality to be used by an identity validation service. The service will review and validate identity and financial information about high-net-worth individuals, adding it to the distributed ledger to confirm they have verified it. A third party, e.g., a bank or financial service provider, can be given secure access to the MDL to confirm that the individual's information has been verified. This validation service will be useful to individuals who need to comply with AML or KYC requirements.

Corporate due diligence specialist — corporate credit: This use case demonstrates the functionality and storage uses that allow companies to use distributed ledgers to validate their identity and report on their finances. A trusted third party reviews the company information and adds it to the distributed ledger, thereby confirming they have verified the information. Potential creditors or business partners are provided with a public key, allowing them to either confirm that the information has been verified, or view the company information itself.

Insurance company — motor policy placement: This use case demonstrates how an individual or business seeking an insurance policy can store their insurance history and relevant data on a distributed ledger and share the key with an insurance company when applying for a new policy, or an endorsement to a new policy. New policy details can be added to the MDL allowing the policyholder to easily request new policies or updates.

Insurance company — small business policy placement: This use case examined how a corporate identity MDL could be used to place a small business policy. The core use case was to consider the interaction of an insurance MDL with a corporate credit MDL, with implied interactions with individual identity MDLs, e.g., a director joining or leaving the corporation.

3.2.2 Assess and appraise

The team and consortium members agreed on the use cases to be tested and what anonymized data could be supplied for the testing. In parallel, the team sought to approach other organizations known to operate distributed ledger systems in order to invite them to participate by providing their distributed ledgers for comparative testing. In the event, Bitcoin data was easily available for analytical comparisons and Ethereum had just launched a new system (Frontier) for which data was readily available. However, three other parties who claimed to have "open source" software proved, despite discussion, not to have software yet ready for comparative testing.

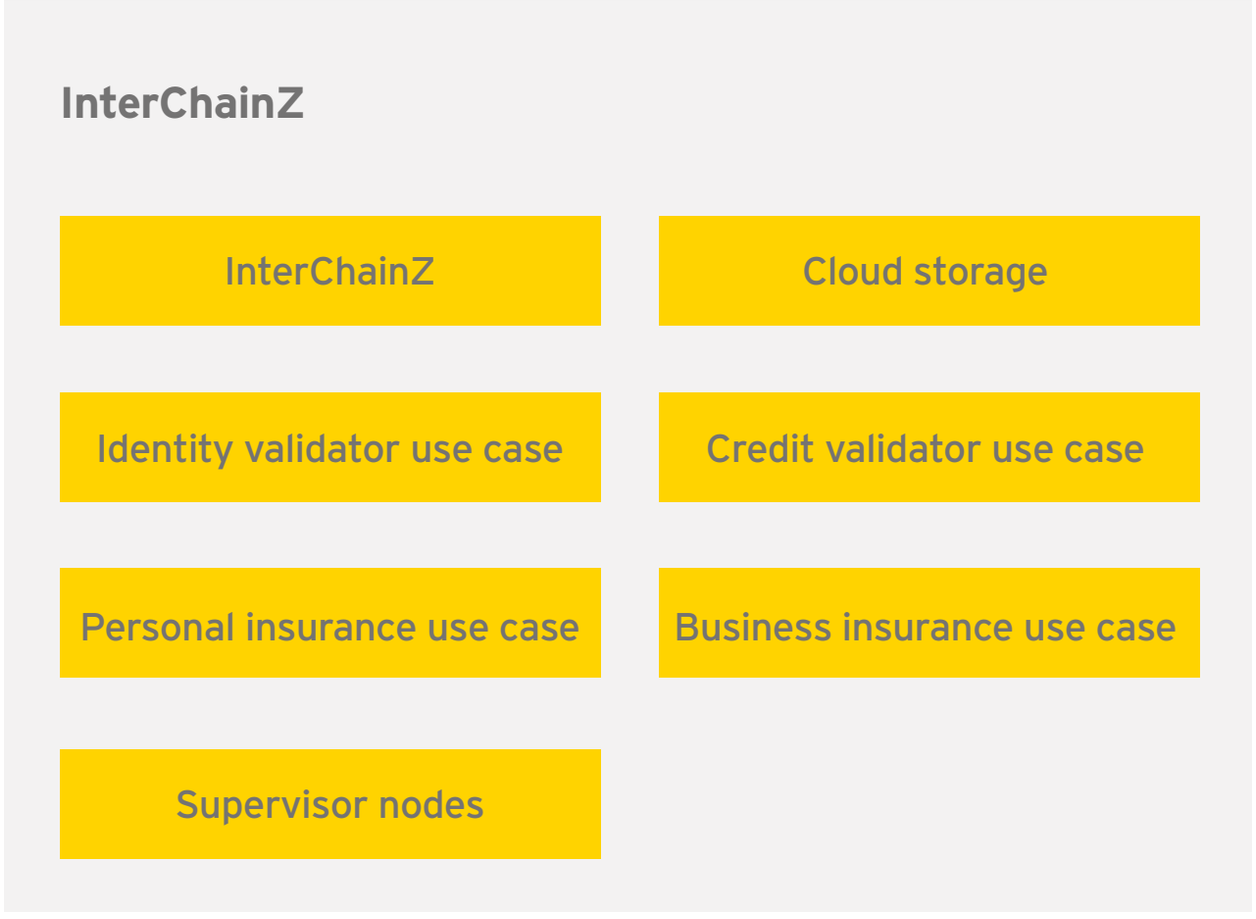
3.2.3 Lookaheads and likelihoods

The third stage of research centered on uploading data for each use case's content MDL and consortium members were invited to explore their use case on InterChainZ. R&D focused on validating three separate architectures, including:

- All nodes – every node (aka server) can add to the MDL
- Master node – only the master can add to the MDL
- Supervisor node – the supervisor needs two other nodes to cosign in order to add to the MDL

An independent ICT expert subjected InterChainZ to a security review during the course of the research, concluding, "the system stacks up cryptographically, by which I mean you can use the system to create the kind of non-repudiatable proof you want." However, the more important the system, the more attractive it becomes to attack.

Figure 3: InterchainZ dashboard



3.2.4 Options and outcomes

In the fourth stage of the research, the team explored storage options and network architectures for InterChainZ. Each use case was expanded to contain not only a content MDL (with all the documents), but also a related identification MDL, with the team exploring different levels of interactions between the two MDLs. The team also sought to test the scalability of InterChainZ by increasing the number of servers across which the prototype runs.

3.2.5 Understanding and undertaking

The team collated preliminary findings stemming from previous stages, including issues and recommendations for future R&D. A user guide was created and circulated to all consortium members. A sensemaking session was organized with the research consortium members to discuss the findings and recommendations and how these should be presented.

3.2.6 Securing and scoring

During this final stage, the team worked to finalize web-based materials including an overview of distributed ledgers, a user guide for InterChainZ, the overall findings, including related videos and graphs, and proposed recommendations for future research.

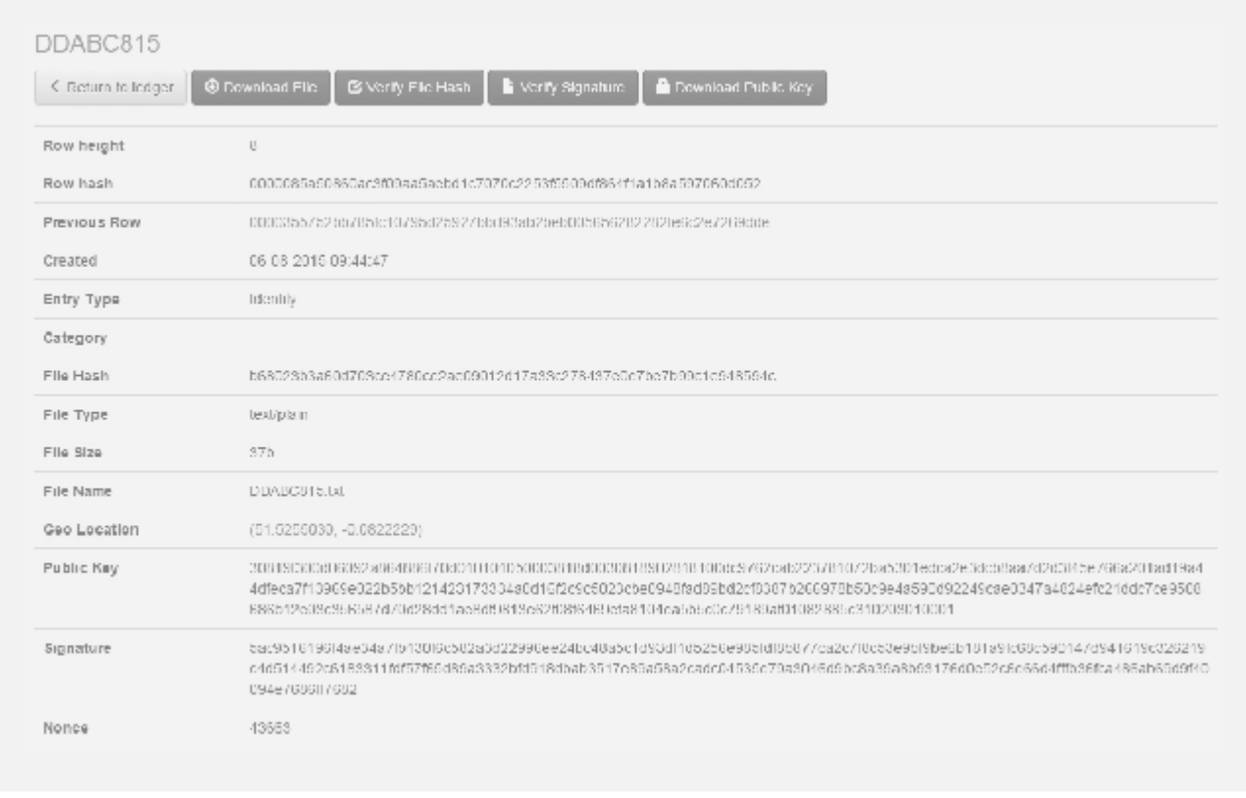
3.3 Technical work

At the top-level, InterChainZ provided access to seven basic "use cases":

- **Deal room (for public demonstration):** single content/transaction MDL; all node validation
- **Credit validator use case (for consortium use):** single content and transaction MDL; all node validation
- **Identity validator use case (for consortium use):** split content/transaction MDL; all node validation
- **Personal insurance use case (for consortium use):** two MDLs, a customer and a company MDL — both of these MDLs are combined content/transaction MDLs; all node validation
- **Business insurance use case (for consortium use):** technically identical to personal insurance use case but uses MDLs distinct from the personal insurance MDLs

- **Cloud storage (for consortium use):** a single transaction MDL; files are stored separately using Amazon; files are encrypted first before being sent to Amazon; uses master node validation
- **Supervisor nodes (for consortium use):** another credit validator use case; single content/ transaction MDL; uses supervisor node validation.

Figure 4: Screenshot of identiy use case



InterChainZ identified a number of potential architectures to manage the addition of data to the MDLs:

- **Free-for-all nodes:** each and every server across which InterChainZ runs has the same level of access to the MDL and the same permission to add to the MDL
- **Master node:** one server is defined as the master and has permission to add to the MDL; all servers including the master can have access to the MDLs and their contents
- **Supervisor node:** any node that wishes to add to the MDL needs two other nodes to cosign; as with the master node architecture, all servers have the same level of access to the MDLs and their content
- **Majority nodes:** a simple majority (51%) of nodes live on the network must co-stamp any addition to the MDL; as with the master node architecture, all servers have the same level of access to the MDLs and their content
- **Collective nodes:** all nodes must co-stamp all additions to the MDL

4. Project learning

4.1 Terminology

Early in the InterChainZ project, it became apparent that the further the discussion moved away from Bitcoins and blockchains, the easier conversations became. Bitcoins and blockchains were burdened with too much baggage. Terminology is evolving rapidly, hence the team's focus on MDLs as the term of choice. Colloquially, the data structures were frequently referred to as "chains" or "chainz." Further, the team emphasized the "boring" nature of MDLs, and that "boring is brilliant." The technical focus might be on boring "ledgers," but the excitement is in the applications above.

4.2 Identity

It also became clear that "identity" issues are universal. One of the great advantages of doing consortium research was that the identity chains were both "use cases" and essential infrastructure that would have had to be built for anything else of substance. Distinguishing "identity" from "transactions" and "content" made processing and distribution sense, at the expense of a bit more complexity in comprehension.

Figure 5: Architectural choices

Option	How it works	Potential benefits	Potential risks	Further thoughts
Master	Specific node must approve all entries	▸ Central ability to control ledger ▸ Straightforward to update approval rules ▸ Increased speed of entry to ledger as no need to wait for other nodes to be live ▸ Simple to implement	▸ Single point of failure – ledgers cannot function without it ▸ Remain reliant on single trusted third party	See cloud storage demo for example
Supervisor	A number of specific nodes must approve all entries	▸ Relatively straightforward to update approval rules ▸ Moderate speed of entry as only waiting for specific nodes	▸ Remain reliant on specific nodes being live ▸ More complex implementation – need to agree supervisors and fallbacks	See supervisor nodes demo for example
Majority	51% or more of nodes must approve all entries	▸ Not dependent on specific nodes to be available	▸ More complex to implement – e.g., to calculate how many nodes are live at any time	To be further developed
Collective	All nodes must approve all entries	▸ Increased certainty over entries – no partial approval allowed	▸ Requires all nodes to be live at all times ▸ Likely to impact performance while waiting for 100% approval	To be further developed
Free for all	Any member of network can add to chain	▸ Simple to maintain and implement ▸ Relatively high performance ▸ Does not require specific nodes to be live	▸ Lack of control over data entry	See client use case demos

While InterChainZ showed that MDLs can work together, and the project explored many different architecture possibilities, what was explored is certainly only a small portion of what is possible. One business area that could use more exploration is whether an MDL system is best as one MDL per entity (person, corporate) interacting with many transaction or content MDLs, or as a set of big MDLs (identity, transaction, content) for a process such as AML, leading to identity information replication on different processes.

4.3 Validation choices

Different business uses probably require different node structures. For example, the master node architecture would be appropriate where a regulator is confirming all transactions in a market as being from valid market participants. The supervisor node architecture might suit a small group of large organizations interacting with multiple smaller ones. While Bitcoin blockchain's "proof-of-work" validation approach is fascinating, one of the basic premises for InterChainZ was to focus on exploring "non-blockchain consensus or identity" MDLs, i.e., what benefits could be achieved when not using currencies or tokens. This decision provoked some external criticism, principally questioning whether there were benefits to MDLs without proof-of-work validation mechanisms.

Brown (2014c) has produced a categorization that starts to make sense of "truthful records" versus "how things are agreed." His diagram shows that there are a number of useful areas where different structures might apply.

The research partners, including the Alderney regulatory observer, contend that regulators are present in most financial markets. Thus, where regulators are prepared to co-stamp transactions, or support co-stampers who provided some trusted third-party elements, tokens are unnecessary. There is evidence of regulatory interest. From 9 July 2015 to 8 August 2015, the States of Jersey held a consultation on "Regulation of virtual currency." That consultation considered "whether there is a case for adopting a standard for distributed ledger technology and the possibility of potential future pan-Channel Island work in this area." In more detail, "whether regulation of the underlying 'distributed ledger' technology would be advantageous in providing confidence to the marketplace that the Channel Islands are suitable jurisdictions in which to conduct 'distributed ledger' technology-based business.

Figure 6: Brown's categorization

		Who do I trust to maintain a truthful record?			
		A central authority	**A group of known actors**	**A group of actors, some known**	**Nobody**
What is the universe of "things" I need people to agree on?	**Ownership of on-platform assets**	Central bank, commercial bank		Ripple (XRP)	Bitcoin
	Ownership of off-platform assets	Custodian bank	Hyperledger	Ripple (Gateways)	Coloted coins, Counterparty
	Obligations and rights arising from an agreement	Clearing house	Eris	Ripple (Codius)	Ethereum

Source: Richard Brown

A standard might involve registration, inspection, certification and periodical checking of the underlying 'distributed ledger' technology system sitting behind any particular business that would use, develop or provide 'distributed ledger' technology" [States of Jersey (2015)].

Nick Williamson and others have introduced a terminology distinguishing "permissionless" ledgers that rely on tokens or incredulous amounts of trust, against "permissioned" ledgers where there are strong structures for multiple parties, e.g., regulators, or the ledger is within a single organization.

Figure 7: Permissionless versus permissioned consensus and trade-offs

	Permissionless	**Permissioned**
Explicit token	**HashCash/proof of work**	**Proof of stake**
No explicit token	***Magic***	**Organization as a blockchain**

Source: Williamson (2015b)

Further, token or coins are expensive. The process of solving the equations needed to maintain a token-based system consumes energy and slows transactions. The approximately 10 minute transaction window of Bitcoin and the seven to 15 second window of Ethereum contrast strongly with the 3,000 to 5,000 transactions per second achieved using InterChainZ's "permissioned" ledgers, i.e., 106 times faster than Bitcoin.

4.4 Content chains

The project developed a number of MDLs that directly stored documents, as well as MDLs that only recorded the "hash" of documents. This led to the development of three conceptual MDLs, "identity chains," "transaction chains," and "content chains." Corporate and individual identity chains authorize access to a transaction chain. A transaction chain holds the core ledger records of all transactions, but only a hash of original documents. The content chain is an MDL holding all of the original documents. The content chain might be managed by a third party for storage and retrieval because of its size. This conceptual structure is quite flexible. The only technical difference between the chains is that the identity and content chains have a fixed-length hash field while the content chain has a variable length field.

In testing, the content chains held a variety of documents, pictures, videos or spreadsheets, from a few thousand bytes up to 100 megabytes. In practice, the numbers are likely to grow rapidly. Just for the personal identity chain, a basic 100 nodes handling 1,000 clients would have a chain (excluding updates and changes) of approximately 75 gigabytes. Moving to a more realistic 500 nodes and 10,000 people gets to 3.75 terabytes, or 500 nodes and 10,000,000 people to 3.75 petabytes. Thus, the ability to segregate the large storage requirement, yet retaining the same MDL architecture, provides an ability to control this increasing size more smoothly. Further, most MDL benefits remain for a content chain under a managed service. Users can still copy it if they wish to. The function of adding new transactions to the content chain can still be transferred easily, preventing permanent centralized control of the content chain by a supplier.

Figure 8: Overview of use cases working together

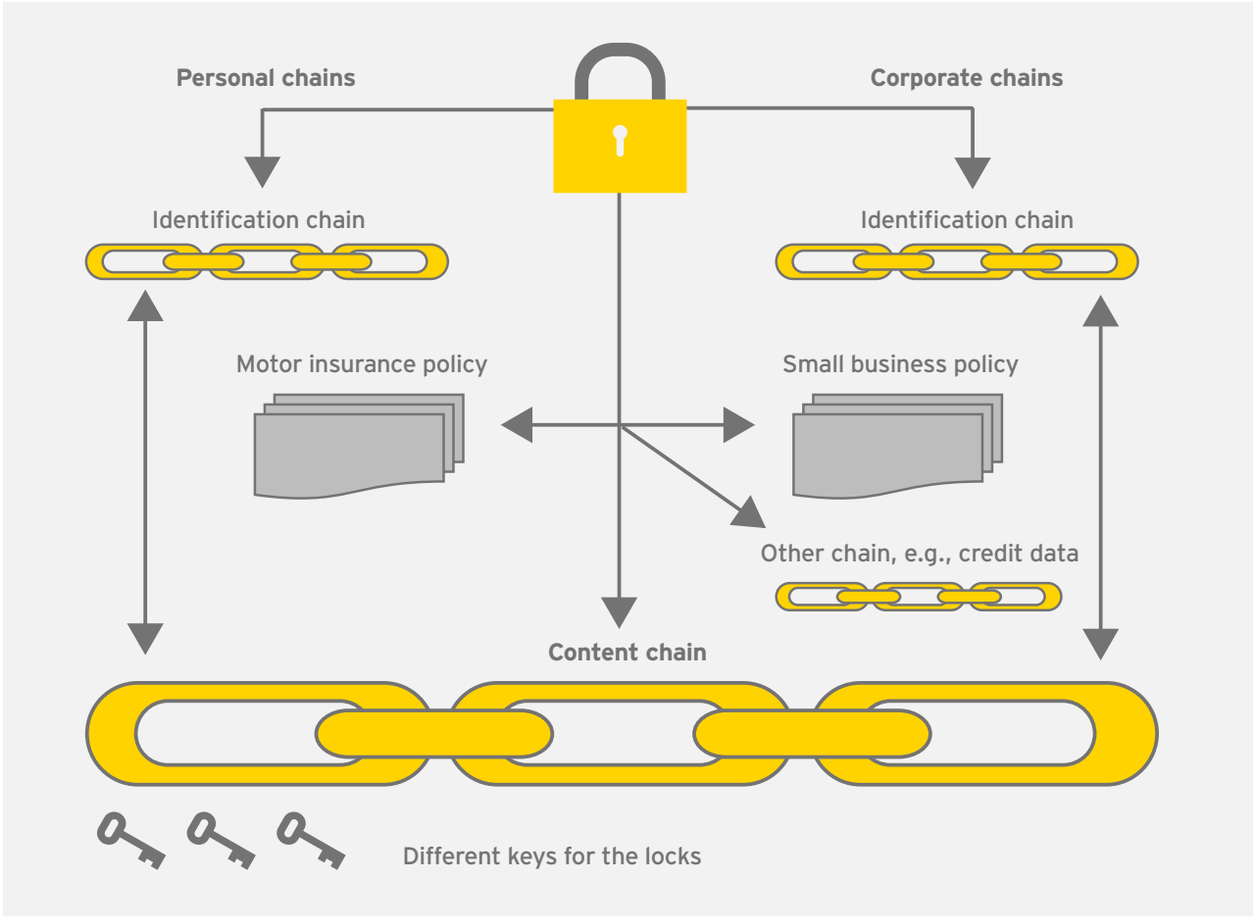


Figure 9: Categorization of chains – one or many chains

Option	How it works	Potential benefits	Potential risks	Further thoughts
Single chain	All content, transactions and identification information is held on one chain	▸ Straightforward data structure, easy to implement and to search ▸ Distribution – all data distributed throughout the chain thus reducing risk of data loss from a small number of nodes	▸ Volume – as chain grows it will require large storage capacity ▸ Performance – likely to impede speed of searches and access ▸ Regulatory – potential lack of oversight over sensitive personal information	Useful for demonstration purposes and for smaller private chains
Dual chains	Separate transaction-content chain and identification chain	▸ Maintains a simple link between data and content ▸ Allows for more options for storing sensitive content, e.g., in stand-alone chain infrastructure, or in tradition storage, e.g., local servers ▸ Lower volume identification chain reducing storage requirements and improving performance ▸ Facilitates giving access to subsets of data	▸ Slightly more complex structure requires security for both chains and links ▸ Regulators and customers may require additional audits to confirm links in place	Need to develop protocols for linking data on chains and retrieving data from content chain
Many chains	Separate content chain, identification chain and transactions chains	▸ As for dual chains, also allows an individual to link to different chains in different networks for different types of transactions, e.g., an insurance chain and a credit chain	▸ Increasingly complex structures may be harder to control ▸ Requires excellent data sharing protocols to validate data links to different chains networks	Business case for additional complexity needs development, may be a longer term option

4.5 Further research

At a basic level, the project showed that MDLs work and can work together, but a number of avenues are yet to be explored, and a lot of essential infrastructure is lacking. Further research could include:

- **Simplify:** market functions (order matching, margining, account functions, clearing, settlement, as well as possible uses of a token currency within exchange) and usability and ergonomics to enhance the end-user experience (exploring the end-user experience by connecting to off-the-shelf wallets for cryptographic key management)
- **Automate:** facilities for automated creation of new mutual distributed ledgers (a parameter driven system providing options for permission management, proof-of-stake and identity settings, supervisor-master and other node settings, "voting" permutations, and peer-to-peer structure settings) and exchange functions (processes to make the basic interacting ledgers into a demonstrator of a full exchange, with numerous "use cases" therein, e.g., sharing identity functions with transactional functions and storing relevant documents securely and permanently)
- **Integrate:** integrity proofing (dynamic anomaly and pattern response additions, monitoring and testing facilities), content hash-addressable storage market (C#ASM) (extending the "identity," "transaction" and "content" chain thinking that emerged from InterChainZ into an indexable archiving system both as a ledger itself, but also supporting other ledgers) and data taxonomies, encryption levels and tracking (how feasible is it to have differently labelled categories and "data boxes" (e.g., health, car insurance, home insurance and driving record on a person's MDL) that can only be opened as a group, to encrypt levels with levels (first order health data perhaps before detailed data), to provide access records (who opened, when), and might homomorphic encryption have a role)
- **Control:** management and control features (management information, performance statistics, visualization) and documentation of standards for MDLs and legal entity identifiers

5. Project reflections

5.1 Everything needs identity and authentication

MDLs could transform the way people manage identities and personal information. Individuals could own their data and no longer need to trust third parties to store or manage their information. MDL identity schemes could empower people with personal data storage and management, permission frameworks for access by third parties such as banks or insurance companies, and even distributed reputation ratings. Such applications could reduce identity and fraud, increase confidence in products and lower rates thus increasing coverage. The concept of never losing data could materially alter the way society views identity, privacy and security.

Identity is fundamental to money. The entry in any ledger is about people — A owes B. Thus, tokens of identity are the basis of currency. Søren Kierkegaard, "doubt everything," reminds us that without risk there is no faith; there can be no faith without doubt. There can be no faith in the community without debt, thus credit and a form of doubt about future repayment are intrinsic to monetary systems.

Identity is not just physical, a DNA or retinal match. Identity is not just about ownership of bank accounts or assets. Our identities are the "chains of our lifetime," binding our past and future with the now. For example, school grades, a driving record, tax payments, are all part of a chain of behavior entangled with a particular human body. Our identities encompass our relationships with other people and institutions. Our identities vary depending on who is identifying. The tax office probably has little interest in people's driving records, but may care enormously about the days they spent out of the country.

Corporate identity is even more complex. The transaction "log" of a company could have constant entries — directors joining and leaving, any employee joining or leaving, purchase orders, invoices, payments, approved persons, inspections, annual reports, audit results, even continuous posting of sales and purchase ledgers, etc. If the transactions are authoritative enough, possibly co-stamped by corporate identity validators (e.g., the DueDil use case in InterChainZ), then perhaps dynamic credit or lending application might arise.

MDL technology and related applications could transform the way we manage digital identity (ID), personal information and history. An ID scheme relying on decentralized MDLs combining a public ledger of records with an adequate level of privacy could rival state-backed identity systems. A number of digital ID schemes are emerging, including OpenID Connect, a protocol combining an identity layer and an authorization server, which allows clients of all types (e.g., developers) to request and receive information about authenticated session and end users across websites and apps without having to own or manage password files. Governments too are trying to set up digital ID systems and authentication processes. The U.K., for example, unveiled Gov.UK Verify in September 2014, a proposed public services identity assurance program that might use a network of trusted and vetted third-party providers instead of relying on a centralized database. Estonia has been operating a national digital ID scheme for a decade and is extending application to foreign nonresidents, which would in effect separate state-backed ID from location. Estonia claims that much of its architecture is comparable to the MDL approach.

The Peruvian economist, Hernando de Soto, points to the importance of widespread economic participation for prosperity and stability, and argues that inclusion starts with participation in an information framework that records ownership of property and other economic information. Once there is strong identity, then there is much stronger lending. The developing world is already a place to look for identity innovation. One such example emerges from Unique Identification Authority of India which everyone in the identity world is watching as probably the largest identity project ever.

Creating a trusted and widespread digital ID system could be technically rather straightforward but socially difficult. Public Key Infrastructure (PKI) and digital certificates were all the rage in the 1990s. Many issues, not least commercial confusion, impeded public understanding. While PKI and digital certificates are functional, widespread use has evaded them, though they have niche applications, often in financial services. Social media networks are trying to make their accounts a form of ID though these generally fail to meet basic trust requirements as most are issued without verification.

It is probably not too much to assert that establishing an efficient identity system is the core global development challenge for MDLs. For the developing world, identity is fundamental to getting onto the ledger in the first place. For the developed world, efficient identity systems are fundamental to efficient financial and trading systems.

5.2 Data non-ownership

The persistence and pervasiveness of distributed ledgers make them ideal for providing a lifetime record. There is a swarm of trial applications being discussed, putting assets onto MDLs — land and property, vehicles, ships, satellites, business ownership/incorporation/dissolution records, regulatory records, tax returns, building and other types of permits, court records, government/listed companies/civil society accounts and annual reports, etc. A swarm of other applications are putting data onto MDLs — contracts, passports and IDs, birth or death certificates, signatures, criminal records, high school/university degrees, professional qualifications, certifications, human resources records, medical records, accounting records, business transaction records, locational data, delivery records, health and safety inspections, genome and DNA, genealogy trees, etc.

An MDL identity scheme could take the form of an application hosted using identity validators (i.e., predetermined experts authenticating documents or information submitted) and identity brokers allowed to cross-reference information securely with other data sources (including governmental ones). The application could enable additional functions including personal data storage, authorized access frameworks for external providers or even reputation ratings. Combining authentication and personal data management functionalities with secure MDLs could lead to new frameworks for identity management. If successful, such identity schemes could remove government monopolies in managing their citizens' identities and data.

At a time where access and control over one's own data are becoming increasingly sensitive, empowering individuals to store, update and manage access to their data seems rather appealing. In InterChainZ, the identity validator is a "co-stamper" of data onto a personal or corporate MDL. The owner of the MDL can include what they like, but if they wish to get other people to accept the data's validity, it needs co-stamping. An identity validator might be a government, an accounting firm or a credit referencing agency.

A simple example might be that an accountancy firm needs to co-stamp the inclusion of an annual report on a corporate identity MDL before other parties would normally accept it. Another example might be that people go to an identity validator to encode biometrics, e.g., DNA, retinal scan, photo, facial scan, finger vein identification, thus time-stamping physical identity. Validators have no further access to the data. However, "the validated" can share the key to their identity MDL with other people and organizations. Others rely upon the fact that the data has been co-stamped by a trusted third party.

InterChainZ provided only a single-level categorization, "entry type," e.g., company accounts or health data. A robust system would need a much richer taxonomy, ideally one that could evolve. For an individual, this could be many layered, e.g.:

- Health: dental, physical, mental, exercise, emergency conditions and treatment records
- Insurance: home and contents, life, travel, etc.
- Driving record

The complexity is obvious if MDLs are going to be used at the individual and corporate levels for widespread use.

MDLs raise an interesting prospect that data may not be "owned" in future. Data might be pervasive, persistent and permanent, yet inaccessible to most, or with the loss of a key inaccessible forever. An identity MDL might have a firm "co-stamping" identity information, yet not having any record or future access. This has attractions for some applications and confidence that data is only accessible by the owner could be important. However, at the same time an MDL runs over traditional concepts of data ownership, such as where is the data. A strict answer to "who is taking care of my data?" on an MDL is difficult. To be fair, many cloud applications have the same problem. An MDL could both help or hinder new data protection requirements such as a "right to be forgotten." Current EU regulations might make it difficult to structure MDLs in such a way that the data is not stored outside the E.U., though it may not be accessible outside the E.U. unless an E.U. individual provides their key.

5.3 10 billion and trillions selling it to the machine

Two inexorable trends increase the tensions in identity, globalization and population. In a globalized world approaching 10 billion people, transactional affordability is crucial to success. A few high-net-worth individuals may justify implementing a complex and costly identity scheme, but the promoters of expensive schemes would be pushing billions of potential customers to the side.

Box 3: IBM-Samsung

"IBM has unveiled its proof of concept for ADEPT, a system developed in partnership with Samsung that uses elements of bitcoin's underlying design to build a distributed network of devices — a decentralized Internet of Things.

The ADEPT concept, or Autonomous Decentralized Peer-to-Peer Telemetry, taps blockchains to provide the backbone of the system, utilizing a mix of proof-of-work and proof-of-stake to secure transactions.

IBM and Samsung chose three protocols — BitTorrent (file sharing), Ethereum (smart contracts) and TeleHash (peer-to-peer messaging) — to underpin the ADEPT concept. ADEPT was formally unveiled at CES 2015 in Las Vegas." [Higgins (2015)]

The increase in connectivity — seven billion phones for seven billion people, and internet-of-things devices estimated by Cisco to hit 50 billion by 2020 — will increase the number of transactions severalfold. Further, global population estimates for 2050 circle around the 10 billion mark. The identity problems increase severalfold. Visa and MasterCard already process 10 transactions globally per person per annum, and they are just one type of international provider. If global payments over the decade come to resemble the U.S. today, with several hundred million online payments per day, we are well onto "tera-transactions-per-day" measures in the next decade.

Transactional affordability will drive a "many uses" approach to get the most out of an expensive process. Both high-net-worth and low-net-worth customers expect global identity, whether it is credit card authorization, payments or health records. Their demands will get stronger as they realize what can be achieved, rather than what has historically been put upon them. They will exclude service providers with onerous identity rituals such as KYC/AML. "Many uses" will in turn drive consolidation toward a few, competitive, global systems.

Leaving aside some interesting by-waters, such as a discussion of a technological singularity or techno-rapture (i.e., when artificial intelligence permits the machines to take charge), one interesting anecdote came up during InterChainZ. There was a discussion with a U.S. insurer about how to insure emerging electricity company products. This insurer had been approached by U.S. energy companies about some of their new services, in particular, services that might offer lower electricity charges if consumers allowed the energy company to switch appliances off and on when needed for load reduction or load balancing. In the U.S., one large area for claims is the loss of freezer contents. The insurer realized that it could share data with the energy company so that, assuming two identical freezer units with different content values, a lower content value freezer would be turned off in preference to a high content value freezer.

Further, the insurer realized that someone coming home to a melted freezer might have three options: (a) claim on their domestic insurance, (b) claim from their electricity provider, and in turn indirectly on their commercial insurance, (c) make a fraudulent claim on their electricity provider. In each case, the complexity of proving the chain of commands to the freezer almost mandates an external, "unowned" MDL as a reliable source of records to make claims efficient and remove fraud.

Autonomous machinery will create enormous markets humans never see. To ensure appropriate management, including liability management, MDLs might be a core technology.

5.4 The Temple & the Souk

At a conference in Germany in 1997, Eric Steven Raymond described the struggle between top-down and bottom-up software design [Raymond (1999)]. He contrasted "happy networked hordes of programmer/anarchists [the bazaar] outcompeting and overwhelming the hierarchical world of conventional closed software [the cathedral]."

So what does the future hold for ledgers? It might be the "temple of financial services" against the "souk of the sharing economies." In the temple, the high priests of the blockchain maximalists and the banking traditionalists wage a schismatic war over "the one true coin." The banking traditionalists believe that these MDL fads too soon shall pass, leaving traditional banking intact. The blockchain maximalists, and adherents to some of the other blockchain services, believe that everything in financial services can be replaced. Each believes that only one ledger can prevail, or from the film Highlander, "there can be only one!"

Out in the souk of sharing economies, there is an explosion of vibrant stalls and frenzied groups of small shopkeepers engaged in animated discussions with clients about a myriad of ways of trading. Shopkeepers and clients are prototyping, experimenting and finally deploying hundreds to thousands of different distributed ledgers. These ledgers are often in the corners of wholesale finance, insurance-linked securities, OTC trading, registries or small exchanges. These small communities typically use private, permissioned, identity-authorized ledgers. Meanwhile, governments try to make taxing the church or the market less slippery, with some governments, such as the Channel Islands, exploring how to evaluate sensibly the hundreds of ledgers that may be brought to them for regulation.

While underdog supporters may root for the souk of sharing economies, there may be room for both. A sensible union would be a few, competing, "blockchain-type" services encircling the globe providing end-of-day validation and recording of transactions, while thousands of MDLs do the busy work of serving thousands of shared economies. In order to provide additional trust, the souks publish a hash of their MDL for additional proof of non-tampering, perhaps storing a daily or hourly hash in Bitcoin's blockchain, Ethereum or another high-trust, permissionless, token-earned MDL. In effect, the merchants of the souk bring their ledgers up to the temple to be validated and timestamped by whichever priests occupy the temple of financial services. It may not be orthodoxy, but it is not heresy either.

5.5 Karmic vertigo, sorcerers' apprentices, and evolution

In many ways, it is appropriate that InterChainZ is a Long Finance project. Long Finance asks, "When would we know our financial system is working?" The pervasive, persistent and permanent nature of MDLs means trying to design data structures that might have to last centuries. There is a parallel from 1999.

The Y2K problem (or millennium bug) began in the 60s, 70s and early 80s (sic — two digits) when computer programmers were chronically short of memory, disk space and processor speed. The differences between that period and today were large. The authors began programming in the mid-70s with a luxurious 4 kilobytes of memory on isolated laboratory mini-computers and are writing this article with gigabytes on networked PCs at home. Programmers were told that systems were being built for a finite period of time and, therefore, used a common trick of only recording two digits for an annual date, which saved significant space on large files. Computations on those files depended on two digits being interpreted as "1900+ two digits" and often resorted to further efficiency tricks such as using 98 or 99 as special triggers or adding extra months and days that don't exist. For instance, 98 might mean end of record and 99 end of file. Clearly, problems arose when the real 1998 or 1999 came along. The Y2K problem had an extra zing that 2000 was a leap year and that many programmers mistakenly thought it wasn't (leap year in every year divisible by four, except when divisible by 100 unless divisible by 400).

A natural human response in such situations is to ask how this could possibly come about and who is at fault before getting on to what can be done about it. A first port of call is the programmers, clearly they built the systems using shortcuts that would not stand the test of time and now they have the audacity to charge for fixing it. However, these systems were almost always built for a finite period of time. In the 70s this time period could be as short as two or three years or possibly as long as five or seven years before "we buy a software package," "we move to a fully relational database," or "we upgrade all our systems." A next port of call is the accountants who left these systems off the books when they were key business assets or failed to fund the asset maintenance costs that should have existed. However, accountants had, and have, great trouble getting sensible lifetimes and valuations for computer-based systems.

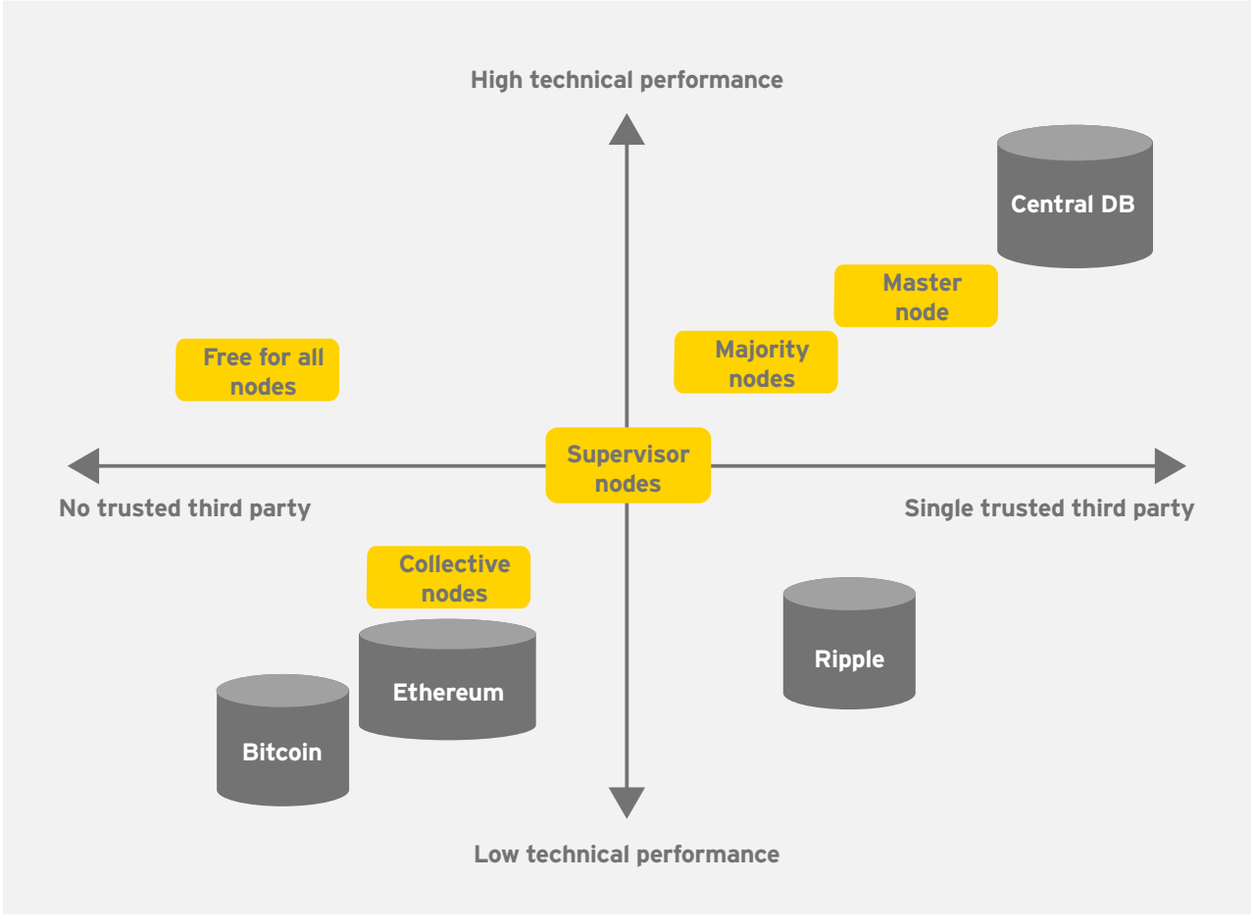
In the event, and at some expense, these systems were successfully upgraded, but the lesson is that discounting the future too rapidly led to modest medium-term gains and long-term costs.

Virtual realist Jaron Lanier applies the idea of "karmic vertigo" to computer code: "The computer code we are offhandedly writing today could become the deeply embedded standards for centuries to come. Any programmer or system designer who takes that realization on and feels the full karmic burden, gets vertigo." Stewart Brand (1999) provides some perspective: "The karmic view of the future can be as distorting as the discounted view. Instead of the reduced responsibility of discounting, karma can impose crushing responsibility, paralyzing to contemplate."

MDLs create a big tension — how to build 100 year pervasive, persistent and permanent data structures and protocols that can evolve. Similar problems have arisen with Hypertext Transfer Protocol (http), with ICANN, and with Bitcoin itself, which in a "sign of the times" is fighting an internal battle to change its protocol to handle a wider range of transactions more swiftly. This short-long, need-for-evolution tension is a big point in favor of semi-centralized solutions such as permissioned ledgers. With a trusted third party and a governance structure, there is some ability to assure the permanence of records, while also being able to update and change entities.

MDLs are sorcerers' apprentices. Once they have been set off, they are hard to rein back or change. For this reason, most people involved with InterChainZ believe that dumb contracts will be the most complicated thing done for some time. While smart contracts are certainly possible, they are not probable, principally because people are unlikely to believe that such contracts can always be safely executed at some point in the future. Interestingly, a full smart contract MDL is "Turing-complete," i.e., can solve any computing problem, or very close to Turing-complete. A Turing-complete MDL could be a giant petri dish to every form computer virus or malware. Proving that a Turing-complete MDL is designed to achieve only its specified objectives is nontrivial. Thus, dumb likely precedes smart by some years.

Figure 10: Low-trust architectures have significant performance costs



5.6 Trust ≈ efficiency

Bitcoin and Ethereum's ability to function in environments of low, zero, or even negative trust, attract attention, even envy. However, overcoming the lack of trust in those environments has a high technical performance penalty. If a "circle of trust" can be established, then transactions within such an environment have a performance advantage. This line of thinking has long been economically interesting (Coase and his followers). Figure 8 attempts to place various types of technical approaches on a scale ranging from "no trust" to a single, central trusted third party.

Concepts of trust arise in many philosophical puzzles that range from Epimenides the Cretan's paradox of "all Cretans are liars" through to Kurt Gödel's Incompleteness Theorem. A paraphrase of Gödel's Incompleteness Theorem applied to trust might read, "We can never find an all-encompassing axiomatic system of trust, without recourse to systems outside it." It seems appropriate to conclude this report on MDLs with Long Finance's Zen koan — "If you have some trust, I shall give you trust. If you have no trust, I shall take it away."

Bibliography

Acord & Equinix, 2014, "Challenge to change part 1 – embracing the economy, poeple and the future of insurance," industry report, Equinix, 1-17
Acord & Equinix, 2014b, "Challenge to change part 2 – the impact of technology," industry report, Equinix, 1-18
Acord & Equinix, 2014c, "Challenge to change part 3 – the future of insurance," industry report, Equinix, 1-19
Adams, J., 1995, Risk, Psychology Press
Allaire, J., 2014, "Thoughts on the New York BitLicense proposal," Circle, 13 August (accessed 14 November, 2014)
Andersen, G., 2015, "A scalability roadmap," Bitcoin Foundation (Blog), 6 October (last accessed 29 September, 2015)
Andreesen, M., 2014, "Why Bitcoin matters," DealBook, The New York Times, 21 January, (last accessed 29 September, 2015)
Antonopoulos, A. M., 2014, Mastering Bitcoin, O'Reilly Media Inc.
Aron, J., 2014, "Bitcoin: how its core technology will change the world," New Scientist, February
Back, A., M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and Pieter Wuille, 2014, "Enabling Blockchain innovations with pegged sidechains," white paper, Blockstream, 1-25
Bank of England, 2014, "Quarterly bulletin," Q3.
Bank of England, 2015, "Bank of England research agenda," discussion paper, February
Baranoff, E., P. L. Brockett, and Y. Kahane, 2014, "1.3 attitudes towards risk," in Baranoff, E., P. L. Brockett, and Y. Kahane (eds.), Risk management for enterprises and individuals v 1.0, Flat World Education
Bazdarevic, N., 2014, "Notre sphère privée est morte: entretien avec Alexis Roussel," InvestNews, September, 20-22
Benedict, K., and P. Abatan, 2014, "Insurance disrupted – crowdsourced policies and social marketing," Cloud Computing Journal, 19 May
Birch, D. G. W., 2015, "What does cryptocurrency mean for the new economy," In handbook of digital currency, Academic Press
Bitcoin Project, 2015, "How does Bitcoin work?" Bitcoin Project, (last accessed 29 September, 2015)
Bitcoin Wiki, 2015, "Scalability," Bitcoin Wiki (last accessed 29 September, 2015)
Blockchain Info, 2015, "Size of the Bitcoin blockchain," Blockchain Info. (last accessed 29 September, 2015)
Cooper, M., 2010, "In search of the eternal coin: a long finance view of history," Long Finance, March, 1-30
Bollen, R., 2013, "The legal status of online currencies: are Bitcoins the future?" Journal of Banking and Finance Law and Practice 24:4, 272-293
Brand, S., 1999, The clock of the long now: time and responsibility, Basic Books
Brown, R. G., 2014b, "Cryptocurrency products and services will determine adoption of the currency – not the other way around," Richard Gendal Brown – thoughts on the future of finance, Blog, 5 October
Brown, R. G., 2014c, "The latest in cryptocurrencies," presentation at the Financial Services Club, 6 October
Brown, R. G., 2014c, "A simple model to make sense of the proliferation of distributed ledger, smart contract and cryptocurrency projects," 19 December – http://gendal.me/2014/12/19/a-simple-model-to-make-sense-of-the-proliferation-of-distributed-ledger-smart-contract-and-cryptocurrency-projects/
Bruce, J. D., 2014, "The mini-blockchain scheme," www.cryptonite.info
BTC Guild, 2013, "BTC's Guild's mitigation plan," Bitcoin Forum, 5 April (last accessed 29 September, 2015)
Buterin, V., 2014, "A next generation smart contract and decentralized application platform," white paper, Ethereum, Ethereum
Buterin, V., 2013, "What proof of stake is and why it matters," Bitcoin Magazine, 26 August

Coinbase, 2014, "Comments on proposed rulemaking regarding regulation of the conduct of virtual currency businesses – DFS-29-14-00015-P," San Francisco: Coinbase, 28 August
De Filippi, P., 2014a, "Legal framework for crypto-ledger transactions,"
De Filippi, P., 2014b, "Tomorrow's app will come from brilliant (and risky) Bitcoin code," Wired, March
De Filippi, P., and R. Mauro, 2014, "Ethereum: the decentralised platform that might displace today's institutions," Internet Policy Review (Alexandre von Humbolt Institute for Internet and Society), August
Digital ID and Authentication Council of Canada, 2015, "Building Canada's digital future," 6 May
Downey, P., 2015, "Registers: authoritative lists you can trust," Government Digital Service Blog, 1 September
El Monayery, R., 2013, "Insurance awareness," The Macrotheme Review 2:7, 147-155
European Union (Parliament and Council), 2009, "Directive 2009/20/EC on the insurance of shipowners for maritime claims," 23 April
Faggart, E., "Bitcoin mining centralization: the market is fixing itself," Coin Brief, 18 June (last accessed 29 September, 2015)
Fargo, S., 2014, "Falling Bitcoin price is the perfect storm for centralization of Bitcoin mining," CCN, 23 September (last accessed 29 September, 2015
FATF, 2014, "Virtual currencies: key definitions and potential AML/CFT risks," Financial Action Task Force, June
Franklin, B., 2012a, "Future risk: how technology could make or break our world," Industry report, The Chartered Insurance Institute, 1-40
Franklin, B., 2012b, "Future Risk: insuring for a stronger world," Industry report, The Chartered Insurance Institute, 1-32
GHash.IO., 2014, "Bitcoin mining pool GHash.IO is preventing accumulation of 51% of all hashing power," GHash.IO. (last accessed 29 September, 2015)
GitHub., 2014, "Blockchain based proof of work," GitHub, March (last accessed 29 September, 2015)
Gittleson, K., 2013, "How big data is changing the cost of insurance," BBC news, 15 November
Glick, B., 2014, "GDS unveils 'Gov.UK Verify' public services identity assurance scheme," ComputerWeekly, 16 September (last accessed 29 September, 2015)
Goldman, Sachs & Co., 2014, "All about Bitcoin," Top of Mind, 11 March, 1-25
Government of Jersey, 2015a, "Views sought on virtual currency regulation," 8 July
Government of Jersey, 2015b, "Consultation on regulation of virtual currency," 9 July
Grigorik, I., 2014, "Minimum viable block chain," Igvita, 5 May (last accessed 29 September, 2015)
Hajdarbegovic, N., 2014, "IBM sees role for block chain in internet of things," CoinDesk, 10 September (last accessed 29 September, 2015)
Hanson, H., K. Rajamani, J. Rubio, S. Ghiasi and F. Rawson, 2006, "Benchmarking for power and performance," IBM Austin Research Lab, The University of Texas at Austin
Higgins, S., 2015, "IBM reveals proof of concept for blockchain-powered internet of things," CoinDesk, 17 January – http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/
Hope, B., and M. J. Casey, 2015, "A Bitcoin technology gets Nasdaq test," Wall Street Journal,10 May
Houses of Parliament, 2014, "Alternative currencies," PostNote, Parliamentary Office of Science & Technology, August
IBM, 2013, "Analytics: the real-world use of big data in insurance," industry report, IBM
ID3, 2014, "21 top Bitcoin and digital currency companies endorse new digital framework for digital identity, trust and open data," press release, 20 October

International Business Times, 2015, "Bank of England: Central banks looking at 'hybrid systems' using Bitcoin's blockchain technology," July 16
Irrerra A., 2014, "UBS CIO: Blockchain technology can massively simplify banking," Wall Street Journal Digits, 27 October
Jelf, O., and S. Seibold, 2015, "Blockchain in the corporate environment has big potential, but faces implementation challenges," Wall Street Journal CIO Report, 27 July
Kaminska, I., 2013, "The problem with Bitcoin," FT Alphaville, 3 March
Kaminska, I., 2015, "On the potential of closed systems blockchains," FT Alphaville, 19 March
Kaminsky, D., 2013, "Let's cut through the Bitcoin hype: a hacker-entrepreneur's take," Wired, 3 May
Knight, C., and A. Butler, 2004, Civilization one: the world is not as you thought it was, Watkins Publishing
Lake, P., and P. Crowther, 2013, "A history of databases," in Concise guide to databases: a practical introduction, Chapter 2, Springer-Verlag
Light, D., 2014, "The internet of things and property/casualty insurance," industry report, Celent, 1-18
Live Work Studio, "Insurance: nobody wants a claim," Live Work Studio (last accessed 29 September, 2015)
Mainelli, M., 2004, "Personalities of risk/rewards: human factors of risk/reward and culture," Journal of Financial Regulation and Compliance 12:4, 340-350
Mainelli, M., 2014, "Infectious transactions from travels abroad," iGTB, June
Mainelli, M., 2015a, "The Temple & The Souk – the future of mutual distributed ledgers," iGTB, July
Mainelli, M., 2015b, "Stranger danger: how to unblock KYC and AML in banks," iGTB, August
Mainelli, M., 2015c, "Unblock the shared economy," Duke Dialogue, Lid Publishing, September
Mainelli, M., and B. McDowall, 2014, "Building bit – what's a poor government to do about AltCoins," Banking Technology, April, 30-33
Mainelli, M., S. Rochford and C. von Gunten, 2011, "Capacity, trade and credit: emerging architectures for money and commerce," report prepared by Z/Yen Group for the City of London Corporation, ESRC and Recipco, December
McAleese, M., 2010, President of Ireland, Remarks to the European Insurance Forum, RDS Concert Hall, Dublin, 30 March
McKinnon, D., C. Kulman, and P. Byrne, 2014, "Eris – the dawn of distributed autonomous organizations and the future of governance," Humanity + Magazine, 17 June
McKinsey, 2011, "Big data: the next frontier for innovation, competition and productivity," industry report, McKinsey Global Institute, 1-156
McMillan, R., 2014, "Hacker dreams up crypto passport using the tech behind Bitcoin," Wired, 30 October
Meetup, 2015, "Bitcoin meetup groups," September (last accessed 29 September, 2015).
Mougayar, W., 2015, "The 3Ps of the blockchain: platforms, programs and protocols," 21 January – http://radar.oreilly.com/2015/01/the-3ps-of-the-blockchain-platforms-programs-and-protocols.html
Nakamoto, S., 2009, "Bitcoin: a peer-to-peer electronic cash system," White paper, 1-9
NewsBTC, 2015, "Deloitte report on central bank owned cryptocurrency," 12 July
New York State Department of Financial Services, 2015, "NYDFS announces approval of first bitlicense application from a virtual currency firm," 22 September (last accessed 29 September, 2015)
New York State, Department of Financial Services, "Proposed New York codes, rules and regulations, Title 23. Department of Financial Services Chapter I. Regulations of The Superintendent of Financial Services Part 200. Virtual currencies," (last accessed 5 October 2015)

Nielsen, M., 2013, "How the Bitcoin protocol actually works," Data-driven intelligence, 6 December (last accessed 29 September, 2015)
OECD, 2006, "The importance of financial education," Policy Brief, OECD, 1-6
Palmer, D., 2014, "Insurance industry 'behind' on harnessing big data," Computing News, 18 August
Polemitis, A., 2014, "Bitcoin series 24: the mega-master blockchain list," Ledra Capital, 11 March (last accessed 29 September, 2015)
Prensky, M., 2001, "Digital natives, digital immigrants," On the Horizon, MCB University Press, Volume 9, No 5. October
PwC, 2014a, "Stand out for the right reasons: how financial services lost its mojo and how it can get it back," industry report, PricewaterhouseCoopers LLP, 1-16.
PwC, 2014b, "Top issues: the insurance industry in 2014," industry report, PricewaterhouseCoopers LLP, 1-44
Raymond, E. S., 1999, The cathedral and the bazaar: musings on Linux and open source by an accidental revolutionary, O'Reilly Media
Reitman, R., 2014, "Beware the BitLicense: New York's virtual currency regulations invade privacy and hamper innovation," Electronic Frontier Foundation, 15 October (last accessed 29 September, 2015)
Rosenfeld, M., 2012, "Overview of colored coins," 4 December (last accessed 29 September, 2015)
Schwartz, D., N. Youngs, and A. Britto, 2014, "The Ripple protocol consensus algorithm," white paper, Ripple Labs Inc., 1-8
Scott, B., 2014, "Visions of a Techno-Leviathan: the politics of the Bitcoin blockchain," E-International Relations, 1 June
Simon, G., 2000, "Insurance: risk sharing," Presentation at the Stern School, New York University , 5 March
Skinner, C., 2014, "There is no next big thing... get over it," Financial Services Club Blog, 25 September
Spencer, R., 2013, "General insurance in the twenty-first century: meeting the challenges," CII Thinkpiece, May, 1-4
Sporny, M., 2015, "An introduction to credentials on the web (video)," YouTube.com, February
States of Jersey, 2015, "Consultation – regulation of virtual currency," part 7: distributed ledger technology standard," July – http://www.gov.je/SiteCollectionDocuments/Government%20and%20administration/C%20Regulation%20of%20Virtual%20Currency%20Final%20Consultation%20Paper%2020150708%20GP.pdf
Swan, M., 2014a, "Blockchain health – remunerative health data commons and HealthCoin RFPs," Institute for Ethics and Emerging Technologies, blog, 29 September
Swan, M., 2014b, "Blockchain: the information technology of the future," compiled by Bitcoin meetup, 1 October
Swan, M., 2014c, "Decentralised money: Bitcoin 1.0, 2.0, and 3.0," Institute for Ethics & Emerging Technologies, 11 November (last accessed September 29, 2015)
Swanson, T., 2015, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems," 6 April
Szabo, N., 1996, "Smart contracts: building blocks for digital markets," Extropy, no. 16
The Economist, 2014, "Estonia takes the plunge: a national identity scheme goes global," The Economist, 28 June
The Telegraph, 2014, "Bitcoin exchange MtGox 'faced 150,000 hack attacks every second'." The Telegraph, 9 March
Vasin, P., 2014, BlackCoin's proof-of-stake protocol v2," white paper

W3C, 2015, "Identity credentials 1.0," Draft Community Group Report, 5 August
Warren, J., 2012, "Bitmessage: a peer-to-peer message authentication and delivery system," white paper, Bitmessage
Williamson, N., 2015a, "What is a blockchain?" 12 April – http://blog.credits.vision/what-is-a-blockchain/
Williamson, N., 2015b, "Permissionless vs permissioned consensus & tradeoffs," 14 April – http://blog.credits.vision/permissionless-vs-permissioned-consensus/
Woo, D., I. Gordon, and V. Iaralov, 2014, "Bitcoin: a first assessment," Bank of America Merrill Lynch, 1-10
World Economic Forum, 2014, "Managing the risks and rewards of big data," The global information technology report 2014: Chapter 1.5, World Economic Forum, 61-66
Wosskow, D., 2014, "Unlocking the sharing economy: an independent review," UK Department for Business, Innovation and Skills, November
Z/Yen Group, 2011, "Capacity, trade and credit: emerging architectures for money and commerce," industry report, Z/Yen Group, London, UK: City of London Corporation, ESRC and Recipco
Zerocash, 2014, "How Zerocash works," Zerocash, 2014. (last accessed 29 September, 2015).

Editorial

The EY Global Financial Services Institute brings together world-renowned thought leaders and practitioners from top-tier academic institutions, global financial services firms, public policy organizations and regulators to develop solutions to the most pertinent issues facing the financial services industry.

The Journal of Financial Perspectives aims to become the medium of choice for senior financial services executives from banking and capital markets, wealth and asset management and insurance, as well as academics and policymakers who wish to keep abreast of the latest ideas from some of the world's foremost thought leaders in financial services. To achieve this objective, a board comprising leading academic scholars and respected financial executives has been established to solicit articles that not only make genuine contributions to the most important topics, but are also practical in their focus. *The Journal* will be published twice a year.

gfsi.ey.com

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY is a leader in serving the financial services industry
We understand the importance of asking great questions. It's how you innovate, transform and achieve a better working world. One that benefits our clients, our people and our communities. Finance fuels our lives. No other sector can touch so many people or shape so many futures. That's why globally we employ 26,000 people who focus on financial services and nothing else. Our connected financial services teams are dedicated to providing assurance, tax, transaction and advisory services to the banking and capital markets, insurance, and wealth and asset management sectors. It's our global connectivity and local knowledge that ensures we deliver the insights and quality services to help build trust and confidence in the capital markets and in economies the world over. By connecting people with the right mix of knowledge and insight, we are able to ask great questions.

The better the question... The better the answer... The better the world works...

EYG No. CQ0316

ey.com

Accredited by the American Economic Association
ISSN 2049-8640