

A REVOLUTION IN TRUST

Distributed Ledger Technology in Relief & Development

"The principal challenge associated with [DLT] is a lack of awareness of the technology, especially in sectors other than banking, and a lack of widespread understanding of how it works."

- Deloitte

Executive Summary¹

In 2016, the blockchain was recognized as one of the top 10 emerging technologies by the World Economic Forum.² The potential of the blockchain and distributed ledger technology (hereinafter "DLT") to deliver benefits is significant. Gartner estimates that DLT will result in \$176 billion in added business value by 2025; that total reaches \$3.1 trillion by 2030.³

Investment in the field reflects the widespread belief that the technology can deliver value. Numerous trials, and some deployments, can be found across multiple sectors.

- Over two dozen countries are investing in DLT
- More than 2,500 patents have been filed in the last 3 years⁴
- As of Q4, 2016, 28 of the top 30 banks were engaged in blockchain proofs-of-concept
- 21 of 63 publicly regulated stock, futures and options exchanges are testing DLT⁵
- The first nine months of 2016 saw \$1.4 billion invested in blockchain initiatives globally⁶
- Venture capital investments in 2016 totalled nearly \$500 million⁷

The Upside

In a recent report, Accenture surveyed cost data from eight of the world's ten largest investment banks, with the goal of putting a dollar figure against potential cost savings that might be achieved with DLT. The report concluded that the banks analyzed could reduce infrastructure costs by an average \$8 to \$12 billion a year. The survey mapped more than 50 operational cost metrics and found the savings would break down as follows:

- 70% savings on central financial reporting
- 30-50% savings on compliance
- 50% savings on centralized operations
- 50% savings on business operations.

The report also highlighted additional benefits, namely increased transparency and better operational data. Given the numbers, it should come as no surprise that interest in the banking and finance sector is high.

¹ The discussion is framed in terms of distributed ledger technology, as opposed to a narrower look at blockchain technology; a broader term that includes solutions beyond the blockchain that have the potential to change the way in which digital assets are created, recorded, transferred, or stored.

² See, http://www3.weforum.org/docs/GAC16_Top10_Emerging_Technologies_2016_report.pdf

³ See, <http://www.zdnet.com/article/executives-guide-to-blockchain/>

⁴ See, <http://pubdocs.worldbank.org/en/710961476811913780/Session-5C-Pani-Baruri-Blockchain-Financial-Inclusion-Pani.pdf>

⁵ See, CoinDesk State of Blockchain 2016.

⁶ See, <https://www.cryptocoinsnews.com/pwc-expert-1-4-billion-invested-blockchain-2016/>

The growth observed in this area in the last few years pales in comparison to the benefits that could be realized when this technology reaches its' full potential. There will be revolutions in payment systems. Money transfers that took days will take minutes. The Internet of Things and self-driving cars will use the blockchain to contract and pay for services. There will be revolutions in business models. In some industries, transaction costs will drop below visible thresholds, unleashing dramatic, sometimes sudden, aggregations and dis-aggregations of business models⁸. DLT evangelists can be heard to say that the impacts may be as great as the original invention of the Internet; as Harvard Business Review recently noted, the evangelists may not be wrong.⁹

Disruptive Properties	Potential Advantages	Key Barriers
<ul style="list-style-type: none"> • Tamper proof record: The system, aided by the use of cryptography, creates a chronological chain of transactional data that is extremely difficult to defraud. • Immutable and transparent: All transactions can be public, traceable and permanent. • Removal of intermediaries: A DLT can remove the need for a third party actor, allowing participants in the network to transact directly. 	<ul style="list-style-type: none"> • Increased Transparency and Openness: A ledger can be open and viewed by any user. It can be a totally transparent record of financial transactions, or of asset ownership and life cycle. • Reduced Transactional Friction: The ledger is owned and maintained by its users, with no need for third party intermediaries, bringing the potential to reduce both transaction times and costs. • Integration of Digital and Physical Assets: Both tangible and intangible assets can be represented on the blockchain. Ownership and life cycle can be traced and, when desirable, the asset can be fully integrated with digital payment mechanisms. • Smart Contracts: Participants in a DLT network can create contractual agreements and embed them into the blockchain where a business logic layer will use triggering events to activate certain actions when pre-defined conditions are met. 	<ul style="list-style-type: none"> • We are still in the early adopter phase of this technology. Best practices, standards and interoperability have yet to be defined. Proven, replicable business models have yet to arise. • Network dependency is a critical failure point. The technology requires Internet access and robust network infrastructure, and that imposes limitations on viability in some markets. • Social, legal, and regulatory frameworks are in their early days and remain an area of uncertainty. • Adequate data storage coupled with an effective means for data retrieval is a necessity. A distributed ledger typically only stores a hash of the transaction data; it is not used for storing the underlying data. • Shortage of DLT-related talent. Recent numbers suggest that hiring in fintech is very difficult at the moment, and that people with DLT skills are in short supply.

⁷ See, <http://www.coindesk.com/research/state-of-blockchain-q4-2016/>

⁸ One could, for example, create an Airbnb-like network, without the need for the company Airbnb.

⁹ See, <https://hbr.org/2017/02/a-brief-history-of-blockchain>

DLT's ability to remove the need for entrenched third-party intermediaries has huge disruptive potential. By replacing the traditional trusted intermediary with a new type of entity -- a peer-to-peer distributed network -- DLT is poised to revolutionize a number of industries, from finance, to legal, to insurance. To the extent that international NGOs function as guarantors of trust -- trust that the funds donated will be used for an appropriate purpose, trust that the aid has been given to the right beneficiaries, trust that the development work that was contracted for was done on time and as specified -- then NGOs too are poised for disruption.

Relief and development's exploration of DLT lags somewhat. There exists significant potential for DLT to deliver benefits for the sector in three broad areas:

1. **New ways to build trust and reduce costs:** Trust is one of the most precious commodities for NGOs. The use of distributed ledger technologies could enhance transparency and accountability and thereby boost trust. Moreover, the use of DLT to facilitate financial transactions and contractual arrangements could reduce transaction costs and promote efficiencies, allowing us to put more of our money to our mission.
2. **New ways to give:** The arrival of digital currencies and the ability to tokenize assets on the blockchain open up new ways for donors to interact with their favorite causes.
3. **New ways to address social problems:** Digital identity management has potential to reduce disenfranchisement and empower individuals to exercise greater control over their identity. DLT and digital currencies also open up new avenues for protecting wealth and facilitating financial inclusion.

Specific applications of interest to relief and development are likely to include:

- Financial Inclusion
- Land Titling
- Remittances
- Enhanced transparency of donations
- Better Beneficiary Onboarding
- Reduced Beneficiary Fraud
- Tracking of support to beneficiaries from multiple sources
- Delivery of social welfare
- Transforming governance systems
- Micro-insurance
- Cross-border transfers
- Cash programming
- Grant management and organizational governance

While the ability of DLT to introduce efficiencies and reduce costs is commonly touted, the larger disruption for our sector may lie in the increased transparency that would result from implementation of DLT-enabled monitoring and reporting systems. The potential exists, for example, to eliminate the fungibility of donations, increasing dramatically the expectations of transparency from donors and supporting institutions and putting new pressures on NGOs to expose their operations to an unprecedented degree. Whether NGOs will welcome this degree of scrutiny, or not, may well be beside the point: If donor expectations shift, the question simply becomes who will manage expectations the best and survive in the new paradigm.

Though it is early days for our sector, the time for exploring the potential is now, lest the early mover advantage inure to smaller, more agile agencies, leaving the bigger players left to play catch-up. The greatest advantages to be gained from implementing DLT solutions are most likely to be achieved by looking at opportunities at a sector level, with an eye towards creating a standardized DLT infrastructure that will enable agencies to build apps and develop use cases that facilitate information sharing and beneficiary tracking across the sector.

Table of Contents

1. An Introduction to Distributed Ledger Technology	6
1.1 The Birth of the Trust Layer	6
1.2 How it works	8
1.3 Smart Contracts	13
2. Noteworthy Applications	15
2.1 Digital Currencies	15
2.2 Banking & Finance	16
2.3 Recordkeeping	17
2.4 Digital Identity	20
2.5 Organizational Governance	21
2.6 Insurance	22
2.7 Supply Chain Management	23
2.8 Voting	24
2.9 Decentralized Exchanges	25
2.10 Commodities	25
3. Applications of Particular Interest to Relief & Development	27
3.1 Crypto-Philanthropy	31
3.2 Financial Inclusion	28
3.3 Cash Programming	30
3.4 Monitoring & Reporting	31
4. Challenges to Adoption & Implementation	34
4.1 Governance	34
4.2 Operational Risks	34
4.3 Compatibility & Interoperability	35
4.4 Risk Management & Regulatory Compliance	36
5. Final Thoughts	37
APPENDIX A - Noteworthy Platforms	43
APPENDIX B - Solutions Providers	46
APPENDIX C - Standards Bodies	51
APPENDIX D - Consensus Methods	54

1. An Introduction to Distributed Ledger Technology

1.1 The Birth of the Trust Layer

The attributes that make distributed ledger technology unique relate to the mechanisms that are designed to assure the trust of the data kept within the ledger. DLT came onto the scene a few years ago with the birth of Bitcoin, but it is not truly a new technology; DLT is an amalgam of proven technologies, combined and applied in a new way. At the heart of any DLT-type system is a mix of long-established concepts like cryptography, ledgers, and databases, as well as more contemporary concepts, like peer-to-peer networks and hash technology; none of these concepts are controversial, or even truly new. What is new is the way these technologies are combined.

Put into a succinct definition, a distributed ledger is a distributed database that maintains a continuously growing list of ordered records.¹⁰ Each participant in the network maintains a copy of the database, and as the database is updated, changes are propagated across the network in near real time.¹¹ Throughout the process, security is maintained by the use of encryption and digital signatures.

In traditional terms, a ledger is a means of recording transactions.¹² Ledgers have existed for thousands of years. Typically, the ledger resided with a single owner and the transactions recorded in the ledger were verified by comparing the data in the ledger to the physical counterparts in the real world, for example, comparing a ledger entry showing the balance in an account to a physical count of the money, or comparing the list of items in the warehouse to an actual inventory of the contents of the warehouse.

“Distributed ledgers – or decentralised databases – 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”

- Richard Brown (Head of Technology, R3)

A traditional ledger needed to be tied to a physical counterpart due to the fact that the ledger had no independent indicia of reliability; it was a single record maintained by a single entity. Trust in the ledger was only valid to the extent to which entries could be corroborated in the physical world by human witnesses.

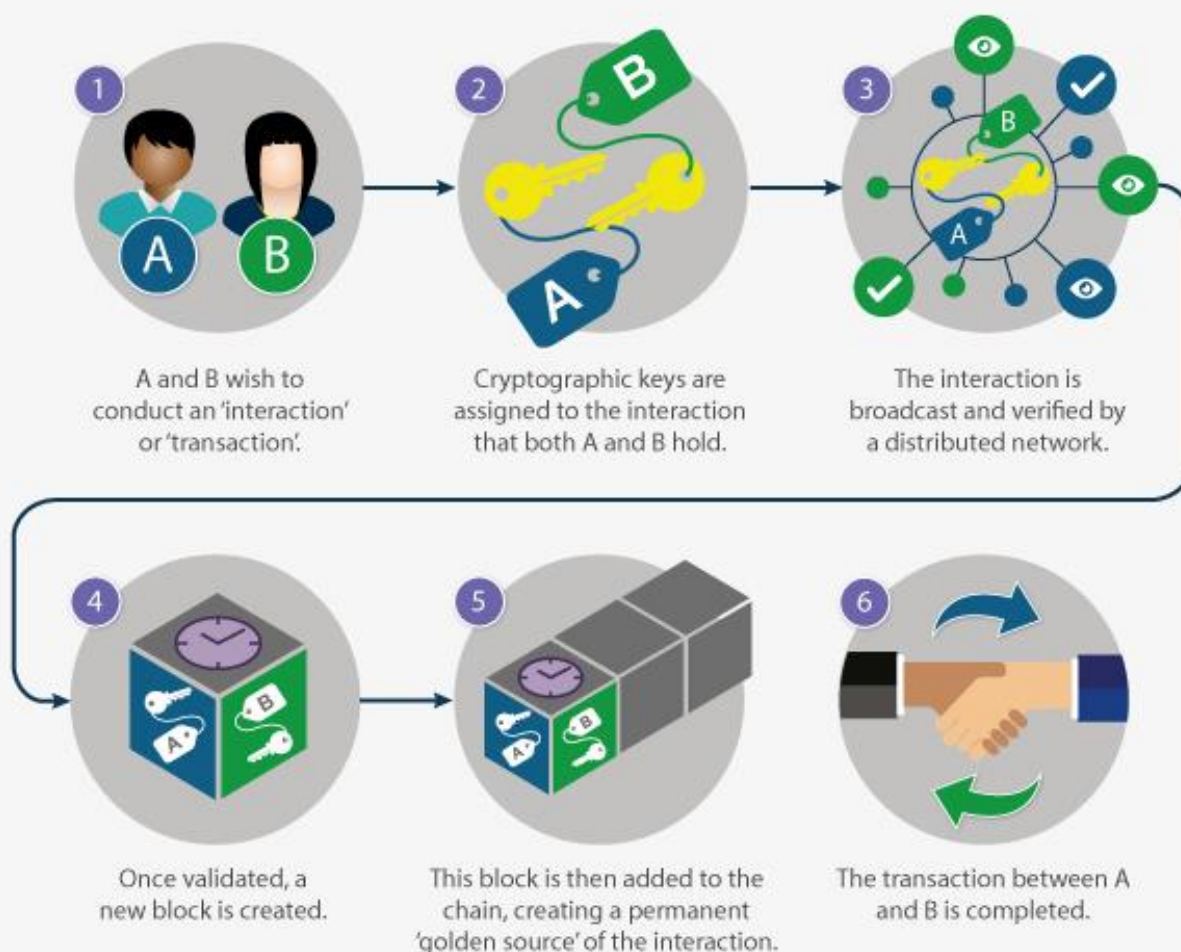
The desire to enhance the ability to leverage traditional ledgers, and to improve the efficiencies associated with validating ledger entries, led to the rise of central authorities in whom parties were willing to trust as intermediaries. Consider the role of banks in a transaction between two parties. If Alice wishes to purchase a car from Ben, she may pay him by means of a check, or by a bank transfer. In either case, Alice needs to initiate the transaction by instructing her bank to make a payment to Ben – who is also typically represented by a bank. Alice’s bank looks at their ledger and verifies that Alice has sufficient funds to make the transfer. Alice’s bank then transfers the funds to Ben’s bank and both banks update their ledgers accordingly. Ben’s bank then notifies Ben that he has received funds. Ben is then able to access the funds via his bank.

¹⁰ See, <https://hbr.org/2017/02/a-brief-history-of-blockchain>

¹¹ There are variations in the implementation in which only portions of the ledger are maintained in any one particular node, in order to maintain scalability.

¹² According to the Oxford Dictionary, a ledger is “a book or other collection of financial accounts.”

How a blockchain transaction works



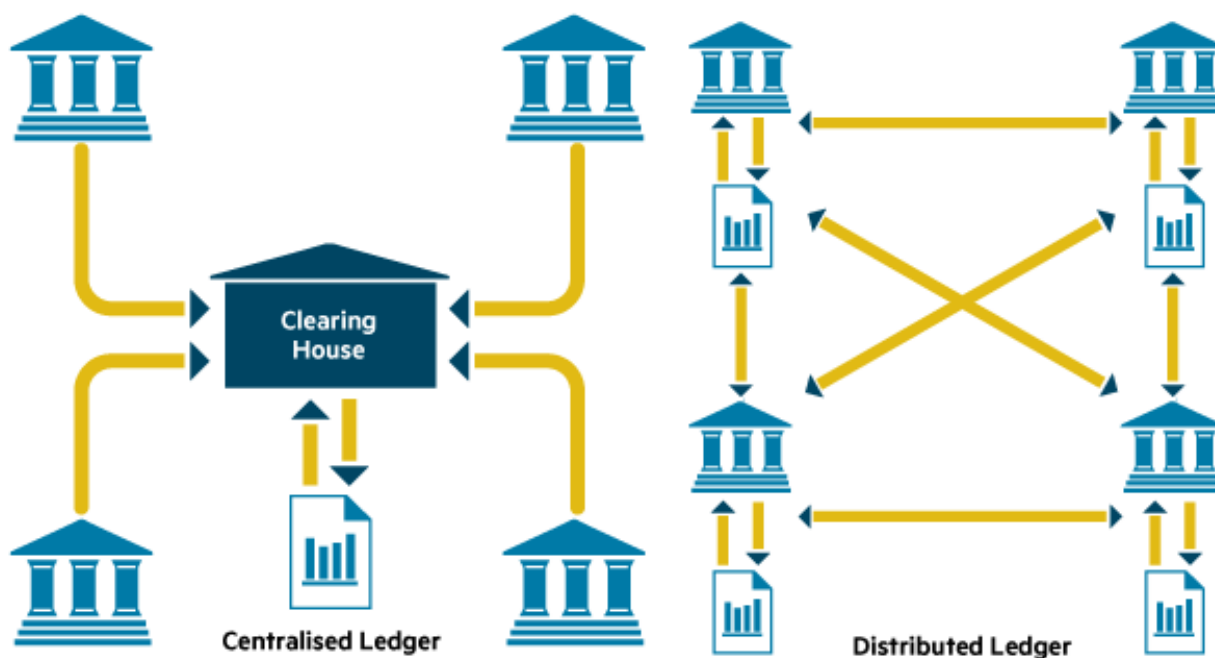
Source: Standard Chartered

This mechanism, where a trusted intermediary is required to represent each party, is so ingrained in various systems that it is all but invisible; it is hiding in plain sight. We ignore the downside; that is, each time an intermediary is added to a transaction, there are additional delays and added fees.¹³ DLT is designed to replace the traditional trusted intermediary with a new type of entity: A peer-to-peer distributed network. This is a key disruptive element of DLT and it signals the start of a new era in network technology, that is, the birth of the trust layer, where peer-to-peer networks, cryptography, and hash technology combine to remove the need for a trusted third-party intermediary.

¹³ The mechanism has become so ingrained in the banking business model that even when a single represents more than one party, there is rarely any reduction in fees or transaction times.

1.2 How it works

At the heart of DLT is a peer-to-peer distributed network of nodes¹⁴, each maintaining a complete copy of the ledger.¹⁵ Unlike a traditional ledger system, no single entity owns the ledger, nor does the ledger reside with only one party. Rather, there are multiple copies of the ledger, each kept by a different node and maintained in synch with the other ledgers in the other nodes on the network.¹⁶



Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

Distributed ledgers generally consist of three logical components:

1. A network of nodes
2. A shared ledger
3. A consensus algorithm

A Network of Nodes

A node is set up on each of the computers participating in the network. The node system operates via a peer-to-peer network (aka, P2P). The network can be vast and widely geographically distributed, but the nodes do need to be able to communicate with each other. A node is typically directly connected to some, but not all, of the other nodes. When one node sends a transaction to its peer nodes, those peers then

¹⁴ When we refer to “nodes” we’re basically referring to the individual computers residing with the participants in the network. The computers are running the software that ties the computer into the distributed network and maintains the local copy of the ledger.

¹⁵ Some DLT systems do not maintain a full copy of the ledger on each node, due to size issues.

¹⁶ Speaking more technically, a DLT system is a service overlay network (SON) in which the nodes process application-specific messages that affect the shared state of the SON.

forward that transaction to other peers, who in turn forward it to yet still others, thereby reaching the entire network of nodes in short order.

The entire system of nodes run a common application that embodies the rules and processes needed for the DLT to work. The nodes communicate actively, based on a set of established procedures by which they exchange transactions, reach unanimous agreement that a transaction can be added to the ledger, and agree on the order in which the transactions are added.

Building a Robust DLT

- The more organizations running nodes in the network, the greater the integrity of the ledger.
- The more active nodes in the network, the more robust the system as a whole.

A Shared Ledger

The shared ledger is the data component that resides in system. The nodes in the network update the data in the ledger and the consensus algorithm ([see](#), below) manages the system to assure that only one true version of the ledger exists.

A Consensus Algorithm

The consensus algorithm sets the rules for the system that determine how the nodes will arrive at a single view of the ledger. Different DLTs use different approaches to consensus¹⁷, but all have the same goals: To make sure that each node is qualified to write their data to the ledger and to assure there is a consistent and trustworthy ledger.

1.2.1 Building a Chain of Blocks

The most common method for implementing a shared ledger is through the use of a blockchain. The term refers to how the data in the ledger is stored. As transactional data is received, it is grouped together into units, called blocks. Each block is then verified and appended to the previous block, thereby creating a chain of blocks. As a block is copied to the chain, it is distributed to all the nodes in the network, thus keeping the copies of the blockchain in harmony.

Each block in the chain carries a unique identifier and is related to the blocks on either side of it. Making a change to any data in the blockchain therefore requires not only changing the block in which the data resides, but also updating all blocks subsequently written to the blockchain. Moreover, if you change the data in one copy of the blockchain, it results in that copy of the chain being out of synch with the other copies of blockchain located on the other nodes in the network -- a result that will lead to the non-conforming blockchain being rejected by the network as invalid. A blockchain creates, in other words, a tamper-evident log. ‘

A block in a blockchain is analogous to a page in a ledger book.

¹⁷ [See](#), Appendix D, below

Blocks, the key structure in a blockchain-based distributed ledger, are simply containers for data. Blocks in any particular blockchain are structured in a consistent manner. The elements of a block typically are:¹⁸

- A unique identifier
- Timestamp
- A link to the previous block in the chain
- Content (that is, the transaction data¹⁹)

1.2.2 Protecting Data and Establishing Identity

Establishing the identities of the participants in the network and their eligibility to participate in the transaction is key to the functioning of any DLT. To that end, DLTs employ a variety of digital identity schemas. Public key infrastructure is widely used, but alternative approaches are also popular.

In addition to verification of identity, the DLT must also be concerned with protecting the data contained in the DLT from fraud or loss. A combination of cryptography and hash technology is employed to achieve the necessary level of integrity and prevent fraud.

Hash technology²⁰ plays a key role in ensuring authenticity. A hash function is typically used to create a unique identifier for transaction data (or documents, or assets)²¹. Hashing a set of data produces a unique “fingerprint” for that data, enabling authentication and helping to establish the provenance of assets.

Once a piece of data is hashed, any change to the data causes the hash value to change. By comparing hash values, any observer can easily detect whether an alteration has been made to the original data. No need to compare every line in a document, or every aspect of a transaction, to make sure it is authentic; with hash technology, you need only run the hash function on the data and compare the resulting hash to the original.

Cryptography is used for...

- Establishing identity
- Signing transactions
- Encrypting data (in transit and/or in storage)

1.2.3 Updating the Ledger

Like a traditional ledger, a distributed ledger is updated whenever a transaction occurs. Updating a distributed ledger requires two key processes to occur:

1. Validation
2. Broadcast and Consensus

¹⁸ Each different blockchain often has different block requirements, typically in terms of the technical data required to be included in each block.

¹⁹ The transaction data is typically not included in its entirety, rather the block contains a hash of the transaction data. And, in this case, the term “transaction” can refer to a variety of objects: traditional cash in/cash out transfers, or a smart contract, or a tokenized asset.

²⁰ A mathematical unidirectional function that summarizes a piece of data, regardless of size, as a short piece of unique data called a “hash value.”

²¹ Hashing has been used for a long time in various database environments, as it is easier to find an item using the short hash key than to search long strings of data.

The mechanics of these two steps varies, depending on the particular DLT in question, and whether the DLT is public or private, and whether the participants in the network are trusted or untrusted.

Validation

The first process is the validation of the transaction. When a transaction is received, it is verified and processed by one or more of the nodes in the network. The validation process undertaken by each node is designed to assure that the contents of the transaction are legitimate. If the transaction data is incomplete or flawed, or the state of the assets do not support the transaction, the transaction will be rejected. If the transaction data validates, then the next step occurs: Broadcast and Consensus.

Broadcast and consensus

Once validated, the transaction data is broadcast to the nodes in the peer-to-peer network. Before the transaction data can be written to the ledger, the nodes must agree on which transactions will be added to the block and in which order. Once an agreement has been reached, then the block will be added to the chain.

The process of reaching agreement among the nodes is known as “consensus.” Achieving consensus in distributed systems is a classic computer science problem and there are many different methodologies for building consensus ([see](#), Appendix D, Consensus Methods).

1.2.4 Correcting Errors

A traditional blockchain is immutable. If an error in a transaction is discovered after the data has already been accepted by the network, the options for correcting the entry are limited to two choices:

- Re-writing the entire blockchain from the erroneous block forward in time to the present;
- Adding a subsequent entry that corrects the prior entry.

Private DLT systems ([see](#), below), are sometimes structured to allow for the correction of errors by trusted participants.²²

1.2.5 Common DLT Variants

Public vs. Private

Also known as “open” and “closed” systems, the labels refer to who has permission to participate in the DLT.²³ A public (or open) system welcomes any participant, and often includes as a feature an option for pseudonymity by the participants. In contrast, a private (or closed) system limits participation to a restricted set of actors – actors that are known and trusted. Not surprisingly, the latter variety seems to be emerging as the preferred approach for most enterprise implementations.

²² Public systems, however, are typically immutable to make fraud more difficult.

²³ While any individual system may be open or closed, participants (nodes) might still be differentiated (or grouped) and assigned varying levels of permissions that allow them to perform only some portion of the functions available. [See](#), “Permissioned vs. Permissionless” (supra).

Strengths and Weaknesses of Public Blockchains²⁴

Strengths	Weaknesses
Immutable ledger	Irreversible transactions
Comparatively fast settlement (relative to a traditional processes)	Slow transaction clearing
Reduced security risks (relative to a centralized system)	More vulnerable to attacks by malicious actors
Easy to audit	Reduced privacy
Reduced need for trust	Higher energy consumption

While Bitcoin, the best-known example²⁵ of DLT, uses a public blockchain, businesses are investing more time and money in the development of private blockchains. Private blockchains are using the same distributed ledger technology to record transaction data, but are doing so within private clouds or virtual environments that are accessible only to the other parties in the network, thereby enhancing security and privacy and providing faster transaction settlement times.²⁶

Permissioned vs. Permissionless

DLT systems, be they open or closed, can either allow each participant to perform all the tasks available (a permissionless system)²⁷, or they may group and restrict the participants' rights and privileges (a permissioned system).²⁸ While permissionless systems are the hallmark of public blockchains, permissioned systems offer high utility value for those that require a way to provide control over important functions. For example, a (hypothetical) DLT system might allow some participants to operate only nodes that read the ledger entries. Another group of participants might be allowed to both read and write to the ledger, while yet a third group can read, write, and issue new assets.²⁹

²⁴ Source: CoinDesk: State of Blockchain Q3 2016.

²⁵ The top three public blockchains are: Bitcoin, Ethereum, and Ripple.

²⁶ The downside most frequently cited is that private systems are less robust, as they rely on fewer nodes.

²⁷ See e.g., Bitcoin is the best known example of a permissionless system.

²⁸ See e.g., The Corda platform is one example of a permissioned system.

²⁹ Similarly, nodes could be added to the system for the specific purpose of allowing regulators access to the data in the blockchain. These "regulatory nodes" would give regulatory agencies the ability to view transaction data in near real time. MIT's Digital Currency Initiative is reported to be working on an "auditable ledger" protocol that protects user privacy while still allowing auditors to see enough information to verify details. See, <http://www.coindesk.com/3-big-blockchain-ideas-mit-working-right-now/>

Permissioned blockchains compare favorably against permissionless systems in several key areas:

Quick comparison of Permissioned vs. Permissionless systems³⁰

	Permissioned	Permissionless
Access	Read/write controlled by permissions	Open read/write
Speed	Faster	Slower
Security	Only approved participants	Open participation
Identity	Known identity	Anonymous/Pseudonymous
Asset	Any asset	Native asset

Permissioned systems are increasingly favored by many firms that are developing business applications that rely on DLT; especially in highly regulated industries, such as banking and finance.

1.3 Smart Contracts

A smart contract is a digitized contract that is stored on the blockchain; it is “smart” because it contains programming logic that can automatically execute the terms of the contract.³¹ Smart contracts can be run on a variety of DLT platforms. While the Bitcoin blockchain provides only limited support for smart contracts, most of the later platforms have made allowances for a business logic layer – a smart contract environment - in their implementation. Ethereum³², for example, provides a fully programmable smart contract environment. The Ethereum system includes an address for executable contract code. When the contract address receives a properly formatted message from a user, or another contract, a node executes the code.³³

By way of example, assume Party A agrees to pay Party B \$1,000 in 30 days, if a set of clearly established conditions are met. The agreement is registered as a smart contract and the terms written to the blockchain. Over the course of the 30 days, as the conditions are met, the party who has been selected to certify that the conditions have been satisfied writes that confirmation to the blockchain, thereby creating a time-stamped, certified record. When the 30 days have passed, the logic in the smart contract looks to see if the conditions have been met, and if so, automatically releases the payment to Party B.

The Downside

While the promise of smart contracts is encouraging, the reality is somewhat grimmer. A recent study of more than 19,000 smart contracts running on the Ethereum platform found that 44% of the contracts contained errors.

The complexity of the system, and the lack of qualified and experienced programming resources, means that contracts often contain errors. The DAO hack that hit a complex smart contract running on Ethereum -- and cost an estimated \$50 million -- is the most well-known of these flawed smart contracts.

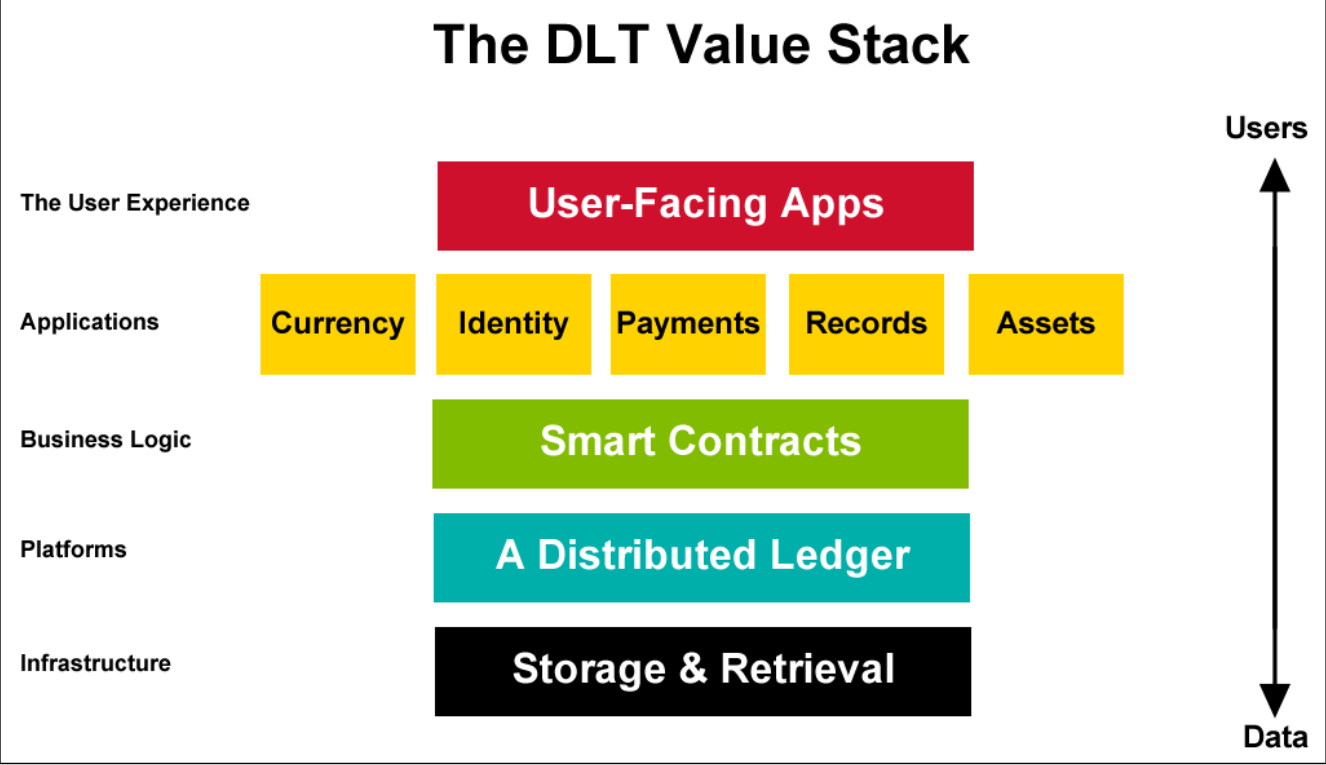
³⁰ See, CoinDesk: State of Blockchain Q3 2016.

³¹ A concept first set forth over 20 years ago by Nick Szabo. See, “Smart Contracts,” Extropy Magazine (Szabo, 1996).

³² See, Appendix A, Noteworthy Platforms.

³³ For a fee, of course! The processing fee is proportional to the complexity of the code and resulting demand on computing resources.

Given that smart contracts function without an intermediary to interpret contract terms and deal with changing circumstances, the application of this technology needs to be assessed and implemented carefully. Smart contracts need to be error free, or at least error tolerant. Given the current state of development, and the fact that complex contracts often require some interpretation, smart contracts are probably best suited for simple contracts with clear-cut provisions.



Given time, the smart contract environment is likely to mature in sophistication. One of the first steps we've seen in that direction is the appearance of multi-sig and time lock contracts. Multi-sig contracts permit the execution of logic when approval is given by one, or more, signatories. Time lock contracts authorize actions to occur only after a specified period of time has passed. Both of these features open the door for some increased ability to react to changed circumstances or incomplete data.³⁴

³⁴ Digital Asset's proposed Global Synchronization Log is another step in the right direction, essentially enhancing smart contract compatibility and increasing the robustness and integrity of smart contract implementations. See, http://digitalasset.com/static/documents/The_Global_Synchronization_Log.pdf

2. Noteworthy Applications

2.1 Digital Currencies

The blockchain concept was originated to facilitate the digital currency Bitcoin. The majority of Bitcoin's progeny followed the same path and employed some variant of public blockchain technology.³⁵

In April of 2017, Coinmarketcap.com identified 699 digital currencies in use today.³⁶ The top five digital currencies, by market cap were:

1. Bitcoin
2. Ethereum
3. Ripple
4. Litecoin
5. Dash

Of those five, all but Ripple run on public blockchains.

Publicly traded digital currencies provide one of the most visible uses of DLT and arguably represent the best-established use case for the technology. These independent currencies have driven development of DLT and have inspired cross-sector innovation.

Central bank-backed digital currencies are relative newcomers but are receiving significant attention from the banking and finance industry.

- In late 2015, Tunisia became the first country in the world to offer a national digital currency, the e-Dinar. Using blockchain tech, the Tunisian government is working to create an expanded ecosystem for using the e-Dinar for mobile banking and a variety of other purposes, from bill payments, to remittances, to payment of wages.³⁷
- Senegal has also released a national digital currency. The currency, known as eCFA, is intended to service not just Senegal, but all of West Africa. The first phase launched in Senegal. The second phase will see the same currency implemented in Cote d'Ivoire, Benin, Burkina Faso, Mali, Niger, Togo, and Guinea-Bissau.³⁸

A Killer Use Case

While there is often talk about how blockchain lacks a valid use case, Bitcoin makes a pretty convincing argument that blockchain tech works. Consider the following facts about the Bitcoin blockchain:

- It handles over 250,000 transactions per day
- It handles between \$195 million and \$378 million in transactions each day
- It manages \$19.6 billion of value
- It has more than 5,400 active nodes

Moreover, since the first block was mined, back in January 2009, the Bitcoin network has never been hacked, subverted, or offline; an enviable record of business continuity. The Bitcoin blockchain is, in other words, both vital and effective.

³⁵ Litecoin, one of the most popular digital currencies, is actually a fork of the Bitcoin codeset.

³⁶ See, <https://coinmarketcap.com/all/views/all/>

³⁷ See, <http://techmoran.com/54824-2/>

³⁸ See, <http://www.financemagnates.com/cryptocurrency/news/senegal-to-introduce-blockchain-based-currency-to-west-africa-ecfa/>

- The Bank of Korea – Korea’s central bank – has announced a partnership with R3 to launch a digital currency.³⁹ The exact scope of the initiative is, at this time, unknown.
- MIT’s Digital Currency Initiative is said to be working on prototyping a central bank-backed cryptocurrency.⁴⁰

Another related innovation is the rise of private cryptocurrencies, typically to facilitate transactions within a private network.

- Citigroup has announced a private cryptocurrency, dubbed “Citicoins.” The Citicoins initiative is focused on payments and elimination of counter party risk when dealing with smaller local banks.⁴¹
- In 2014, Goldman Sachs announced “SETLcoin,” which they label a “cryptographic currency for securities settlement”.⁴²
- UBS, Deutsche Bank, Santander, and Bank of New York Mellon are also brewing their own cryptocurrency, a digital cash instrument called the Utility Settlement Coin which “will pave the way for disruptive change in the way we process securities.”⁴³
- The Bank of England has announced RSCoin, a digital currency that will initially be aimed at exchanges and clearinghouses, with possible future expansion into the consumer sector.⁴⁴
- Finally, the People’s Bank of China (PBOC) announced in December, 2016 that they had completed proof of concept testing of a digital currency that will initially be used by the banking sector. The PBOC has hinted that the currency may be the beginning of a move toward the digitization of the Renminbi.⁴⁵

2.2 Banking & Finance

The banking and financial services sector is not only one of the earliest adopters of DLT but also one of the most advanced in application. A 2017 survey of executives at financial institutions by Bain and Company found that 80% of the executives believe “DLT will be transformative and will significantly impact markets, and a similar percentage expect their organisations to begin using it before 2020.”⁴⁶

Though the sector was an early mover, the highly regulated nature and traditionally conservative culture of banking and finance has meant that actual systems in production are few. Among the notable exceptions:

- In late 2015, Nasdaq released the Linq platform – a blockchain powered system for issuance of private securities.⁴⁷

³⁹ See, <https://www.cryptocoinsnews.com/korean-central-bank-deploy-r3s-blockchain-proof-concept/>

⁴⁰ See, <http://www.coindesk.com/3-big-blockchain-ideas-mit-working-right-now/>

⁴¹ See, <https://thenextweb.com/worldofbanking/2016/09/16/how-blockchain-is-transforming-business-models>

⁴² See, <https://themerkle.com/top-5-cryptocurrencies-under-development-by-central-banks/>

⁴³ See, <http://www.ozy.com/rising-stars/cashing-in-on-cryptocurrency-in-hong-kong/69686>

⁴⁴ See, <http://www.telegraph.co.uk/business/2016/03/13/central-banks-beat-bitcoin-at-own-game-with-rival-supercurrency/>

⁴⁵ See, <https://www.cryptocoinsnews.com/chinas-central-bank-completes-digital-currency-trial-blockchain/>

⁴⁶ See, http://www.bain.com/images/BAIN_BRIEF_Blockchain_in_Financial_Markets.pdf

⁴⁷ See, <http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326>

- The Commonwealth Bank of Australia, UBS and Santander are using the Ripple protocol to transfer payments, saving both time and money.⁴⁸
- American financial services company Northern Trust Corporation has launched the first functioning private equities blockchain in partnership with IBM and a client equities fund in Sweden.⁴⁹ The system employs Hyperledger's Fabric⁵⁰ platform. Each member of the equities fund runs their own node, with a separate regulatory node being deployed for the local regulator to observe transactions in real time.

Among the initiatives currently under development, but not yet deployed:

- A post trade financial services platform that will move \$11 trillion in credit derivatives to a custom built distributed ledger system. The system was commissioned by the Depository Trust and Clearing Corporation (DTCC) and is being built by Axoni, in consultation with R3. The system has passed proof of concept and is currently under development.⁵¹
- A DLT system for handling transactions between corporate treasuries and financial institution at Bank of America Merrill Lynch.⁵²
- Several consortia are working on DLT solutions aimed at the traditional trade finance model. The Hong Kong Monetary Authority, together with multiple banking partners, is currently exploring this area.⁵³ The group's efforts focus on applying DLT solutions in three areas: Smart contracts, tracking transactions statuses, and matching invoices to purchase orders.
- The pressure to come up with affordable solutions to stricter KYC (Know Your Customer) requirements is driving a number of financial institutions to explore digital identity management. Efforts typically focus on digitising customer records and documents so that they can be updated and shared among banks through a DLT platform. A number of firms are working in this area (see, Sec. 2.4, below).
- South Korea's Financial Services Commission has announced plans to launch a blockchain-powered pilot project for financial services. The announcement was made in January of 2017; details remain scarce.⁵⁴

2.3 Recordkeeping

Recordkeeping taps the blockchain for its power as an activity register and an aid to authentication and provenance. The immutable nature of the blockchain provides a powerful tool that allows you to verify the

⁴⁸ See, <https://thenextweb.com/worldofbanking/2016/09/16/how-blockchain-is-transforming-business-models>

⁴⁹ See, <http://blogs.wsj.com/cio/2017/02/23/northern-trust-deploys-blockchain-for-private-equity/>

⁵⁰ See, Appendix C.

⁵¹ See, http://hub.digitalasset.com/hubfs/Press%20Releases/PRESS_RELEASE_DTCC_Digital_Asset_Repo_Release.pdf

⁵² See, <http://newsroom.bankofamerica.com/press-releases/corporate-and-investment-banking-sales-and-trading-treasury-services/microsoft-and-ba>

⁵³ See, http://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf

⁵⁴ See, <https://www.cryptocoinsnews.com/report-south-korea-to-launch-full-scale-blockchain-financial-services-pilot-in-2017/>

state of a piece of data at a particular time.⁵⁵ Moreover, if the data changes over time, you can create a record of the evolution of the data, easily viewable by participants in the network.

The leading player in this space is Factom; they have created an open source DLT that uses blockchain tech to provide a permanent, time-stamped record of data⁵⁶. Clients subscribe to the service to get access to the system and, for a fee, can publish encrypted data to the Factom blockchain as needed. As the blockchain is immutable, the data is verifiable and auditable, creating a trail for proof of process or other compliance needs. In their largest project to date, Factom has been retained by the U.S. Department of Homeland Security to provide data infrastructure for U.S. Customs and Border Protection. The Factom blockchain will be used to secure the storage of the large amount of data collected daily by a multitude of Customs and Border Protection security cameras, sensors, and internal databases.

Other notable initiatives in this area include:

- The U.S. Government recently awarded \$600,000 in blockchain-related development grants aimed at applications relevant to record-keeping intensive health care industry. The focus of the effort is on how DLT technology can be used for secure record keeping for patients.⁵⁷
- In another healthcare-related initiative, the Philips Blockchain Lab⁵⁸ is embarking on an exploration of how DLT can be used to manage health care records via the Tierion platform⁵⁹. Tierion allows easy integration of web and mobile applications for data gathering; the data is then stored on the blockchain as irrefutable proof of the time and contents, thereby giving all parties a verifiable record.
- SAP Ariba, which connects 2.5 million buyers and sellers around the world, has announced a blockchain-based recordkeeping system to track and reveal documents related to the movement of goods. The system is being developed in conjunction with Hyperledger.⁶⁰
- China's Alibaba has partnered with OnChain, an open-source blockchain developer in Shanghai, to launch a DLT product named Law Chain. The product offers an email repository that allows participants to store critical email data (via hash values) on a blockchain. Should a conflict arise, the users can download the emails. Given that the emails are logged and timestamped on the blockchain, and that the contents can be verified by comparing hash values, the system opens up the potential for emails to be accepted as evidence in Chinese courts of law.⁶¹
- Estonia launched the e-Estonia initiative, with a plan to move a large number of personal records, including all health care and prescription data, into digital records protected by a combination of blockchain technology and public key infrastructure.⁶²

⁵⁵ As noted elsewhere in this paper, excepting special situations, the data itself is not written to the blockchain, rather a hash of the data is stored, along with a time stamp.

⁵⁶ The Factom blockchain piggybacks on the Bitcoin blockchain. Factom records the state of their blockchain in the Bitcoin blockchain every 10 minutes. See, <https://www.factom.com/about/faqs>

⁵⁷ See, <https://today.law.harvard.edu/feature/new-technology-block/>

⁵⁸ See, <http://www.usa.philips.com/healthcare>

⁵⁹ See, <https://tierion.com/>

⁶⁰ See, <https://www.forbes.com/sites/tomgroenfeldt/2017/03/22/sap-ariba-will-use-blockchain-to-track-shipments-ensure-authenticity/#200345785082>

⁶¹ See, <http://www.financemagnates.com/cryptocurrency/innovation/alibaba-deploys-onchains-antshares-blockchain-for-super-secured-email/>

⁶² See, <https://e-estonia.com>

- Similarly, Dubai has launched a citywide blockchain strategy with a stated goal of being “the first Blockchain-powered city by 2020.”⁶³ The Dubai blockchain strategy has three prongs: Government efficiency, industry creation, and thought leadership. The Dubai government estimates its blockchain strategy has the potential to generate \$1.5 billion each year in savings from document processing alone.⁶⁴
- Cook County in Illinois is home to the second largest land title registry office in the USA. The office is testing the use of the Bitcoin blockchain for transferring and tracking property titles and other public records.⁶⁵ The system will handle title applications and the filing of liens with the resulting output considered to be part of the public record.⁶⁶
- In March, 2017, Sweden concluded the second phase of a blockchain land registry trial. The system is designed to provide a secure process for real estate transactions and mortgage deeds and is predicted to save taxpayers over \$100 million a year in costs.⁶⁷
- In contrast, the state of Vermont attempted to move land title registry onto the blockchain without success, stating that the cost of implementation outweighed the potential benefits.⁶⁸
- The Republic of Georgia has partnered with BitFury to move land titling on to the blockchain, reducing transaction time and dropping per transaction costs from between \$50 and \$200 to \$0.05 and \$0.10.⁶⁹
- A DLT can function as a decentralized credentialing system, where the network acts as the provider of trust, creating a tamper proof verifiable system for registering academic, professional, or workforce credentials. MIT is working on the BlockCerts⁷⁰ system to provide academic credentialing on the back of the Bitcoin blockchain.
- A number of companies⁷¹ are working on solutions that allow artists and creators to claim ownership or attribute authorship with unique IDs and digital certificates of authenticity. Such a system uses a DLT to create an immutable record of the item with can then be used to prove provenance, authenticity and chain of ownership. An added advantage of such a system would be ease of integration with digital payment processes and escrow services.

⁶³ See, <https://www.1776.vc/sdo-blockchain-challenge/>

⁶⁴ See, http://www.smartdubai.ae/dubai_blockchain.php

⁶⁵ This usage is also of interest to relief and development, as lack of access to property title is an issue for many people in informal economies, rendering their largest source of capital essentially inert and ineligible for use in obtaining lending.

⁶⁶ See, <https://bitcoinmagazine.com/articles/chicago-s-cook-county-to-test-bitcoin-blockchain-based-public-records-1475768860/>

⁶⁷ See, <https://cointelegraph.com/news/blockchain-land-registry-trial-in-sweden-concludes-second-phase>

⁶⁸ See, <http://www.coindesk.com/report-blockchain-record-keeping-system-too-costly-for-vermont/>

⁶⁹ See, <https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#ce1c6884da3>

⁷⁰ See, <http://blockcerts.org/>

⁷¹ See e.g., Ascribe, <https://www.ascribe.io/> and Verisart, <http://www.verisart.com/>

2.4 Digital Identity

The ability to prove one's identity is a fundamental need in any system and is a critical element in many humanitarian relief situations. The World Bank estimates that up 2.4 billion poor people worldwide lack official identification.⁷² The problem extends, however, beyond the poor and disenfranchised. In a variety of transactions, there is increasing pressure from authorities for information that satisfies know your customer (KYC) and ultimate beneficial owner requirements. Those requirements are leading to increased costs and burdens associated with establishing identity with legal certainty. An International Chamber of Commerce survey in 2016 found that 90% of the businesses surveyed considered anti-financial crimes compliance to be a significant impediment to trade.⁷³

A decentralized personal data management system employing DLT could provide an alternative to the traditional trusted identity authority; an authority that is typically associated with a sovereign government and therefore some times absent or disrupted in emergency and disaster situations. The refugee plight in Europe highlights the problem of those caught "in-between" and of traditional systems overwhelmed by the volume of stateless individuals.

An authoritative decentralized identity system that exists outside the control of a state government could, for the first time, effectively place records in the control of the individual, thereby facilitating the fluid movement of individuals between physical borders and political systems.

Given the key role identity plays in a wide variety of contexts,⁷⁴ it is perhaps not surprising that there are a number of actors attempting to craft solutions that employ DLT. The graphic, below, shows one commentator's⁷⁵ recent effort to document the identity start-up landscape. 189 identity start-ups span seven segments of the market.

Questions Remain

Despite the enthusiasm across the industry, significant questions remain regarding the viability of digital identity schemas, including:

- Viability in low bandwidth environments
- The risk of vendor lock-in
- Compatibility and interoperability
- Security and privacy

⁷² See, <http://www.worldbank.org/en/topic/ict/brief/the-identity-target-in-the-post-2015-development-agenda-connections-note-19>

⁷³ See, <https://cdn.iccwbo.org/content/uploads/sites/3/2016/10/ICC-Global-Trade-and-Finance-Survey-2016.pdf>

⁷⁴ Including the anti-money laundering (AML) and know your customer (KYC) functions that are increasingly critical in banking and finance.

⁷⁵ See, <https://oneworldidentity.com/identity-startup-landscape/>

Identity Startup Landscape



Source: One World Identity (<http://oneworldidentity.com>)

The most noteworthy success in this area is Estonia. Since 2007, Estonia has been successfully operating a universal digital identity scheme using the blockchain.⁷⁶ All government data concerning an individual is kept on the blockchain, and controlled by the individual. The identity scheme lies at the heart of the system and enables a low-paperwork approach to documentation that relies on digital signatures.⁷⁷ The system is so successful that a number of non-Estonians use the system to manage their digital signatures as well.⁷⁸

2.5 Organizational Governance

The American state of Delaware is home to more than 66% of the companies in the Fortune 500 and also home to 85% of initial public offerings (IPOs). In 2016, state authorities began to move aggressively towards adopting DLT to streamline corporate governance procedures in the state. Delaware's goal is to enhance document filings, data retention, and compliance by means of a system that combines DLT and digital signatures. Among the initiatives currently underway:

- Migrate the Public Records Archive to a distributed ledger to automate compliance with state document retention and destruction rules.
- Issue legally-enforceable smart UCC filings
- Distribution of shares via DLT

⁷⁶ The Tunisian government is exploring a similar project using a combination of mobile technology and DLT to manage government identification documents. See, <http://techmoran.com/54824-2/>

⁷⁷ See, <http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge>

⁷⁸ See, <https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world>

- Expanding registry services to include features not presently available⁷⁹

The transparency that comes with DLT creates new opportunities for corporate and governmental governance. Companies like Otonomos⁸⁰ are focused on using DLT to automate the process of forming, funding and governing a company. Other players, like BoardRoom⁸¹, are working on providing a complete blockchain-based governance platform for organisations.

While DLT seems set to enhance traditional corporate governance, it has also given rise to a new type of corporate entity, the Decentralized Autonomous Organization (“DAO”).⁸² A DAO is a type of corporate organization that uses the blockchain to replace traditional corporate functions. A DAO is run entirely through rules encoded into smart contracts. In its’ most extreme form, a DAO could run completely independently of human management.

The DAO concept is testing the boundaries of corporate law and securities regulations. The exact legal nature of an entity formed in this manner is still up for debate, and at least one attempt at creating a DAO resulted in the loss of \$50 million in investor value.⁸³

2.6 Insurance

Insurers, like banks, are intermediaries and hence have much to be gained by embracing DLT. In a recent study, McKinsey stated “the blockchain has huge potential to enhance insurers’ business models.”⁸⁴ An August 2016 study from PwC found that reinsurers who embrace blockchain could reduce expenses 15-25%, saving \$5-10 billion a year.⁸⁵ McKinsey identified the following areas where DLT could disrupt insurance:

- Automation by smart contracts
- Easier fraud detection
- Increased pricing effectiveness
- Reduction of administrative costs⁸⁶

DLT could also reduce the difficulties attendant to microinsurance.⁸⁷ As an arbitrator of trust, it would enable insurance participants in remote locations to enter into contracts with confidence. The low costs of buying and registering insurance contracts on the blockchain, then enabling them via smart contracts, would reduce transaction costs to levels that would make microinsurance practical, even in remote locations.

⁷⁹ See, <http://www.coindesk.com/what-expect-delaware-blockchain-initiative-2017/>

⁸⁰ See, <https://www.otonomos.com/>

⁸¹ See, <http://boardroom.to/>

⁸² Also sometimes referred to as a “DAC” – a Decentralized Autonomous Corporation.

⁸³ Despite the uncertainty, and one very high profile failure, there are DAO success stories. The digital currency Dash is set up as a DAO, and seems to be running without controversy or undue risk exposure.

⁸⁴ See, <https://digitalinsurance.mckinsey.com/the-promise-of-blockchain/>

⁸⁵ See, <http://www.pwc.com/gx/en/financial-services/publications/assets/blockchain-for-reinsurers.pdf>

⁸⁶ See, <http://www.mckinsey.com/~media/McKinsey/Industries/Financial%20Services/Our%20Insights/Blockchain%20in%20insurance%20opportunity%20or%20threat/Blockchain-in-insurance-opportunity-or-threat.ashx>

⁸⁷ See, <https://techcrunch.com/2016/10/29/blockchain-is-empowering-the-future-of-insurance/>

Among the firms taking an active interest in the technology:

- The Blockchain Insurance Industry Initiative (B3i) is a consortium of insurance companies collaborating to explore the ability of blockchain technologies to increase efficiencies in the exchange of data between reinsurance and insurance companies.⁸⁸ A proof-of-concept pilot transacting reinsurance contracts between members is expected to be completed by June 2017.
- One of Japan's largest property insurers, Sampo Japan Nipponkoa Holdings, has announced the development of a DLT platform for derivatives. They are also reported to be working on a system for buying and selling insurance policies related to natural disasters.⁸⁹
- Allianz has announced successful completion of a proof of concept using smart contract technology for transacting a natural catastrophe swap. The test run demonstrated transactional processing and settlement between insurers and investors. Allianz states, processing "could be significantly accelerated and simplified by blockchain-based contracts."⁹⁰
- Dynamis is developing a P2P supplemental unemployment insurance that uses smart contracts built on Ethereum to automate underwriting of policies and claims process.⁹¹
- AIG is studying how blockchain can improve the quality of data-driven decision making.⁹²
- Lenderbot is a proof of concept microinsurance initiative by Stratumn, in collaboration with Deloitte and Lemonway. The Lenderbot app enables custom insurance via social media.⁹³

2.7 Supply Chain Management

DLT has the ability to increase transparency in supply chain management by providing a visible ledger of transactions relating to asset ownership, condition, location, and more. Using a distributed ledger, one can register goods and track the transactions that would allow you to trace the goods, identify the parties involved, and track other meaningful data points relevant to managing a supply chain. A complete chain of custody could be exposed via DLT. Depending on the implementation, the record could be made available in near real time, supporting stronger collaboration, increased auditability, and better data intelligence.

IBM estimates that applying DLT to the global supply chain could generate in excess of \$100 billion in improved efficiency annually.

Two IBM projects give some insight into the potential.⁹⁴ Retail giant Walmart has been testing a DLT solution for tracking pork from Chinese farmers to stores in China. In another test, the system is being used to track produce from Latin America to stores in the United States. In a separate trial, shipping giant Maersk worked with IBM to implement a system for tracing containers, with the goal of bringing all the various

⁸⁸ See, <http://www.insurancejournal.com/news/international/2017/02/06/440629.htm>

⁸⁹ See, <https://www.raconteur.net/business/blockchain-for-stronger-links-in-insurance>

⁹⁰ See, <http://www.agcs.allianz.com/about-us/news/blockchain-technology-successfully-piloted-by-allianz-risk-transfer-and-nephila-for-catastrophe-swap/>

⁹¹ See, <http://www.dynamisapp.com/>

⁹² See, <https://www.raconteur.net/business/blockchain-for-stronger-links-in-insurance>

⁹³ See, <https://news.bitcoin.com/stratumn-deloitte-blockchain-bot/>

⁹⁴ See, <https://nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html>

participants in the process on to the blockchain: Customs officials, tax officials, health inspectors, port officials, etc.⁹⁵ The system is currently being trialed on shipments between Rotterdam and Newark.

Several DLT start-ups are also working in the supply chain management space. All of these firms offer the tracking of physical assets using DLT. Among the notable initiatives:

- In January 2017, The Seam, a commodities trading and agribusiness software provider, announced the formation of a blockchain consortium for the global cotton industry. Working with IBM and Hyperledger, the company intends to lead an industry-wide collaboration initiative to create a supply chain and trading ecosystem using DLT.⁹⁶
- Wave⁹⁷ is working on a DLT solution for bills of lading, allowing all participants in the supply chain interact directly, without the need for central authority, thereby removing documentation delays, decreasing costs, and improving transparency.
- Other firms, notably Everledger⁹⁸ and Provenance⁹⁹, are focused on tracking the provenance of products, which can help organizations comply with regulatory mandates and maintain certifications.

2.8 Voting

DLT provides a mechanism whereby electronic or online voting can be coupled with digital identity management and cryptography to help ensure that election results are accurate and honest. Traditionally, votes are recorded, managed, counted and checked by a central authority. A DLT-enabled e-voting schema could empower voters to do these tasks themselves by allowing them to hold a copy of the voting record. The historic record would be immutable as voters could see that any changed voting record was out of synch with other copies of the record. As the European Parliament Research Service observed, such an approach “would shift power and trust away from central actors, such as electoral authorities, and foster the development of a tech-enabled community consensus.”¹⁰⁰

Several countries have begun testing various approaches to e-voting. The Liberal Alliance party in Denmark used a blockchain voting system in 2014 to good effect.¹⁰¹ Estonia has also been an early mover; however, trials revealed a variety of security holes that have caused further assessment.¹⁰² Norway cancelled their trials of e-voting over security concerns.¹⁰³

⁹⁵ A study conducted by Maersk in 2014 found that up to 30 people and organizations are involved in the shipment of a product in a container, resulting in over 200 separate interactions, and a massive pile of paperwork. Maersk found that the cost of the paperwork often equals to cost of moving the shipping container.

⁹⁶ See, <https://www.theseam.com/blockchain/>

⁹⁷ See, <http://wavebl.com/>

⁹⁸ See, <https://www.everledger.io/>

⁹⁹ See, <https://www.provenance.org>

¹⁰⁰ See, [http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA\(2016\)581918_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA(2016)581918_EN.pdf)

¹⁰¹ See, <https://bitcoinmagazine.com/articles/blockchain-technology-key-secure-online-voting-1435443899/>

¹⁰² See, <https://e-estonia.com>

¹⁰³ See, <http://www.nasdaq.com/article/6-blockchain-applications-that-go-beyond-bitcoin-cm716269>

Among the other efforts in this area:

- One of Nasdaq's latest initiatives aims to migrate shareholder proxy voting onto a blockchain solution. Nasdaq successfully tested the system in Estonia, concluding: "While e-voting technology may not be the next killer app, it is very much a practical, necessary, solution that has many potential applications around the world."¹⁰⁴
- Follow My Vote¹⁰⁵ provides a blockchain solution for tracking votes and assuring the integrity of election process.
- Ballotchain¹⁰⁶ piggybacks on the Bitcoin blockchain to enable online voting with high indicia of reliability.

2.9 Decentralized Exchanges

One of the distinctive aspects of DLT is that it is asset-agnostic. Just as you can use a hash value to represent a document or a transaction, you can also use a hash value to represent an asset. This characteristic opens the door for assets to be represented on a ledger by a digital token, which can then be traced and traded.

Asset exchanges – particularly those on a large scale – typically require the intervention of a third party, like a broker, to match the buyer and seller and handle aspects of the transaction. A DLT employing asset tokenization would allow a buyer and seller to work directly, without an intermediary. Additional escrow functionality, managed by the network, could be used to provide the necessary protection for the buyer and seller.

Counterparty¹⁰⁷ is one of the leaders in this space. The Counterparty platform piggybacks on the Bitcoin blockchain, enabling anyone to tokenize an asset and register it on the blockchain. Counterparty's smart contract implementation allows buyers and sellers to place orders and make offers without an intermediary. An escrow system and a strong digital identity schema work together to handle the payment according to the terms agreed to by the buyer and seller.

2.10 Commodities

DLT holds promise in the paperwork-heavy, multi-party world of commodities. European banking giants ING and Societe Generale recently completed testing of a new platform called Easy Trading Connect. The platform was designed to expedite oil trading. A trial showed that the system was able to reduce transaction times from three hours to 30 minutes, producing considerable cost savings for the participants.¹⁰⁸ The trial was more than mere proof of concept, as the system actually handled a shipment of African oil that was traded three times en route to China. The system included traders, banks, an agent, and an inspector.¹⁰⁹

¹⁰⁴ See, <http://www.nasdaq.com/article/nasdaq-successfully-completes-blockchain-test-in-estonia-20170123-00431>

¹⁰⁵ See, <https://followmyvote.com>

¹⁰⁶ See, <http://www.reply.com/en/content/ballotchain>

¹⁰⁷ See, <http://counterparty.io/>

¹⁰⁸ See, <http://www.coindesk.com/major-banks-use-blockchain-prototype-for-live-oil-trade/>

¹⁰⁹ <http://www.coindesk.com/overtaking-banking-race-blockchain/>

While the system is targeted at oil trading, the commonalities that exist in other commodity transactions means that this approach will scale.¹¹⁰

- Uphold¹¹¹ takes a broader approach, acting as a facilitator for purchase or conversion of any form of money or commodity using digital currencies.
- Other players are working the retail side of the commodities field, enabling users of digital currencies to easily make purchases of commodities, particularly gold and silver bullion.¹¹²

¹¹⁰ In a similar trial, Commonwealth Bank of Australia and Wells Fargo recently processed and executed a shipment of cotton from Texas to China using DLT. See, <http://www.cnbc.com/2016/10/24/major-banks-blockchain-trade-cotton-in-a-move-that-could-transform-a-major-industry.html>

¹¹¹ Previously known as “Bitreserve.”

¹¹² See e.g., Amiga Metals, <https://www.amagimetals.com/> or Bitgild, <http://www.bitgild.com/>

3. Applications of Particular Interest to Relief & Development

3.1 Crypto-Philanthropy

A number of the more tech savvy charitable organizations are currently accepting Bitcoin. The early charge was led by those for whom the use of cryptocurrency was a logical extension of their preference for digital liberty, for example the Wikimedia Foundation¹¹³ and the Mozilla Foundation¹¹⁴. Over time, more traditional organizations have experimented with Bitcoin as part of their fundraising strategy. A number of the larger NGOs are currently accepting Bitcoin, including United Way,¹¹⁵ Greenpeace,¹¹⁶ the American Red Cross,¹¹⁷ and Save the Children.¹¹⁸ What little data there is to date suggests that the volume and amount of the donations has been low, raising questions about whether the benefits of accepting Bitcoin outweigh the costs associated with setting up the mechanisms needed to support a new channel for donations.

One of the key arguments against accepting Bitcoin, or any digital currency, is volatility. Of course, volatility works both ways. A donation of \$100 in Bitcoin in January 2016 would have been worth \$349 just one year later.¹¹⁹ Moreover, if an agency wishes to avoid the volatility problem, there exist multiple settlement systems that allow for instantaneous conversion of digital currency donations to fiat currency.

Several organizations have been created specifically to enable merchants, or charities, to accept digital currencies without having to carry to risk of volatility.¹²⁰ The companies act as intermediaries between NGOs and donors who prefer to give using digital currencies. The organizations accept donations in digital currency and then pay out fiat funds.

Direct Giving

One of the most hyped advantages of DLT in philanthropy is the promise of direct giving, whereby donations go directly to beneficiaries using digital currencies (or vouchers). The major selling point being that funds are tracked continuously from donor to end beneficiary using a DLT registry.

Missing the Point?

While there are few fundraising success stories to report, focusing purely on dollar amounts may be missing the point. AJ Leon of the digital agency Misfit, characterizes it as follows:

"Bitcoin is simply a canvas that has emerged. Nascent technologies supported by counter-cultural communities are the most powerful opportunities for us to leverage as fundraisers. Simply by accepting Bitcoin, you're signaling to an entire demographic of well-connected, affluent technophiles that you are one of them."

¹¹³ See, <https://wikimediafoundation.org>. See also, https://wikimediafoundation.org/wiki/Ways_to_Give#Bitcoin

¹¹⁴ See, <https://www.mozilla.org/>. See also, <https://donate.mozilla.org/en-US/give-bitcoin/>

¹¹⁵ See, <https://www.unitedway.org/get-involved/ways-to-give/donate-bitcoin>

¹¹⁶ See, <http://www.greenpeace.org/usa/greenpeace-now-accepting-bitcoin-donations/>

¹¹⁷ See, <https://bitpay.com/520663/donate>

¹¹⁸ See, http://www.savethechildren.org/site/c.8rKLIXMGlpI4E/b.6151527/k.CBE4/Other_Ways_to_Help.htm

¹¹⁹ The other side of the coin would be a \$100 donation in December of 2013 would have been worth approximately \$30 one year later!

¹²⁰ A similar service is offered by several exchanges, see e.g., [Coinbase.com](https://www.coinbase.com)

One firm working on this model is **Helperbit**.¹²¹ The group allows donors to give using their choice of fiat currency or Bitcoin. The organization promises that donors will be able to decide how their donation is used and that the system will make a complete audit available to donors.

Micro-Donations

DLT reduces costs and friction for processing payments, making micro-donations more practical and opening up expanded possibilities for people to make small donations as part of other transactions. The Penny for London campaign is one example of how this can work. The campaign allowed people to voluntarily sign up to donate a few pennies each time they used their Oyster card (stored value card) to make a purchase.¹²² While launched with much fanfare, the initiative failed, eventually raising only a fraction of the fundraising goal. According to those behind the project, signups never reached the necessary number to make the initiative sustainable.¹²³ The mechanism employed by the system, however, worked fine.

Donation of Digital Assets

The ability to tokenize assets expands the possibilities for donors to give assets. Once an asset is registered on the blockchain, a smart contract can be used to define the asset's usage requirements and split the proceeds resulting from use between multiple parties. A donor could, for example, donate intellectual property to an NGO. A smart contract could define limitations on the usage of the IP and dedicate a percentage of royalties earned from that asset across its lifespan (regardless of ownership) to the NGO.

Charity Coins

Several projects have arisen with the intention of harnessing the power of crypto-currency for charitable causes; none have yet to capture the market's attention in any meaningful fashion. Clean Water Coin¹²⁴ claims to be the first crypto-currency developed to be a nonprofit foundation.¹²⁵ As participants in the network mine and use coins, 0.1% of each transaction is donated to a charity wallet and from there distributed to the designated charity.¹²⁶ GiveCoin¹²⁷ is a project from the Strength in Numbers Foundation.¹²⁸ The project has launched a crypto-currency named 2Give. The currency is coupled with Do a Bit of Good,¹²⁹ a charitable giving hub based on Bitcoin. Users can download a screensaver that will then mine Givecoins when the computer is idle, contributing the resulting coins to the associated charity.¹³⁰

3.2 Financial Inclusion

Mobile banking, coupled with DLT payment solutions, opens up new access routes for unbanked populations. There are 3 billion people in the world, mostly in developing economies, who have no access to the financial

¹²¹ See, <https://www.helperbit.com>

¹²² See, <http://www.mayorsfundforlondon.org.uk/news/penny-for-london/>

¹²³ See, <http://www.thirdsector.co.uk/penny-london-closes-having-raised-just-3000-25m-year-target/fundraising/article/1410140>

¹²⁴ See, <http://www.cleanwatercoin.org/>

¹²⁵ As of April, 2017, there is no discernable volume associated with this coin.

¹²⁶ At this time, the designated charity is CharityWater.org.

¹²⁷ See, <http://2give.info/>

¹²⁸ See, <http://strength-in-numbers.org/>

¹²⁹ See, <https://doabitofgood.com/>

¹³⁰ A look at CoinMarketCap.com shows that, as of March 2017, Givecoin's daily volume is essentially zero, having peaked at almost \$8,000 a day in July of 2015.

services that most people in developed countries take for granted. The unbanked have no credit cards, bank accounts or securities trading accounts.

Many of those unbanked consumers, however, have a smartphone in their pocket.¹³¹ In the same way that these consumers leapfrogged landlines to get 4G smartphones, they are likely to leapfrog bank branches and plastic cards to get mobile, low-cost, DLT-based financial services.¹³² As per the Consultative group to Assist the Poor (CGAP), for people living in rural areas on less than \$2.5 a day, mobile money is emerging as a common source of financial inclusion.¹³³

“The very powerful thing about bitcoin in general and specially the technologies behind it, is they are essentially leapfrogging all the technology and providing a new system for processing these huge amounts of transactions for very small costs.”

– Kosta Peric, Bill and Melinda Gates Foundation

The use of digital currencies via mobile wallets can make it easier to get money directly into the hands of the unbanked without the necessity of exorbitant transaction fees. In early 2016, the UK Government Office of Science issued a lengthy report in which they singled out the potential of DLT to reach the unbanked. In the report, they envision how DLT could revolutionize the distribution of welfare¹³⁴:

*Digital identities could be confirmed through distributed ledgers running on securely-encoded devices — or even through software on a mobile device — which would allow end-users to receive benefits directly, at reduced transaction costs to banks or local authorities. This may allow them to become more fully included in the financial system through a secure distribution point that is more reliable than a bank account. Such a solution could also be linked with other systems to reduce the level of fraud and official error in the delivery of benefits, as identities would be more difficult to forge. Such activities may help to achieve one of the DWP’s principal policy objectives: to lift people sustainably out of the cycle of poverty and state dependence.*¹³⁵

DLT offers a number of options for enhancing financial inclusion. In addition to enhancing identity management (see, Sec. 2.4, above), remittances, mobile payments, and solutions that enable micro-finance are leading the way in this field.

Remittances provide one of the strongest use cases for digital currencies. Given the large number of players, and often unattractive fees that go with traditional remittance systems, digital currencies have high utility value, acting as an intermediary currency at much lower costs. Rather than using something like Western Union, an individual can buy Bitcoin (or another digital currency), transfer the Bitcoin to the recipient, who then converts the Bitcoin into the fiat currency of their choice. In addition to significantly lower fees, the transaction can be accomplished very quickly compared to traditional approaches. Companies like Rebit¹³⁶ and BitPesa¹³⁷ are aimed at this new model for remittances.

¹³¹ Many, but not all, particularly in some of the more remote areas where Mercy Corps operates.

¹³² See, <http://www.nasdaq.com/article/op-ed-the-venture-capital-perspective-on-blockchain-technology-cm752490#ixzz4ZqfdUnwJ>

¹³³ See, <http://www.cgap.org/data/financial-inclusion-insights-2015-mobile-money-data>

¹³⁴ The UK report on the potential of DLT to reach the unbanked reflects the technology environment relevant to beneficiaries in the UK. For beneficiaries located in more remote locations with less mature infrastructure, issues remain in terms of overcoming “last mile” hurdles to reach beneficiaries. Even when the infrastructure exists and the technology is in the hands of the beneficiaries, there may still be issues related to establishing pools of liquidity that enable beneficiaries to convert digital currency into fiat.

¹³⁵ See, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

¹³⁶ See, <https://rebit.ph/>

¹³⁷ See, <https://www.bitpesa.co/>

Other initiatives that are aimed at enhancing financial inclusion include:

- **The Bill and Melinda Gates Foundation**¹³⁸ is heavily involved in financial inclusion initiatives, with significant initiatives dating back almost 10 years. The Level One project is looking at how blockchain can facilitate a multi-country, multi-currency remittances system.¹³⁹
- **The U.S. Development Lab**¹⁴⁰, from USAID, is involved with testing digital payments to improve financial inclusion in India.
- **Oradian**¹⁴¹ partnered with Stellar to connect over 300,000 Nigerians with microfinance institutions.
- A number of firms are offering products aimed at re-making the remittances market, including, Ripple,¹⁴² Regalii¹⁴³ and WorldRemit.¹⁴⁴ These products all strive to make it easy for people to send money anywhere, at extremely low costs, often by means of digital currency. In all these cases, while the products are having an impact on remittance markets, more remote locations have yet to see the benefits due to lack of infrastructure and the challenges of maintaining local pools of liquidity.

Crypto-Libertarianism

One of the more interesting experiments in using DLT to enhance financial inclusion is the FairCoin project (<http://faircoin.org>). FairCoin is a cryptocurrency that was purpose built to support cooperative inclusion. The coin uses a unique consensus algorithm known as Proof-of-Cooperation, designed to reward promoting FairCoin and improving operations. The coin is idealistic in its approach and geared to emphasize low impact and low costs. The project seeks to bypass normal markets by jumpstarting and facilitating alternative economic systems, like local mutual credit systems.

3.3 Cash Programming

Cash Programming is one of the hot topics in the relief and development world. While DLTs and digital currencies offer advantages that enhance asset preservation, cross border transfers, and remittances, leveraging those technologies within the environmental constraints that normally accompany cash programming efforts can be challenging.

The World Food Programme is a leader in this area, having recently completed a successful test in Pakistan that used the Ethereum blockchain to manage distribution of cash assistance. Using a smart phone on site, WFP personnel authenticate and record transactions using the Ethereum blockchain. The system also implements biometric scanning to reduce fraud and enable the tracking of how the aid is spent. The WFP program, named Building Blocks, is now moving on to full scale implementation.¹⁴⁵ A new test is slated to

¹³⁸ See, <http://www.gatesfoundation.org/What-We-Do/Global-Development/Financial-Services-for-the-Poor>

¹³⁹ See, <https://www.technologyreview.com/s/604144/how-blockchain-can-lift-up-the-worlds-poor/>

¹⁴⁰ See, <https://www.usaid.gov/GlobalDevLab/>

¹⁴¹ See, <https://oradian.com/>

¹⁴² See, <https://ripple.com/>

¹⁴³ See, <https://www.regalii.com/>

¹⁴⁴ See, <https://www.worldremit.com>

¹⁴⁵ See, <https://futurism.com/blockchain-is-helping-us-feed-the-worlds-hungriest-families/>

kick off in May 2017 in Jordan. The programs plans to distribute an unknown amount of dinars to 10,000 beneficiaries, with a goal of expanding to program to 500,000 recipients by 2018.¹⁴⁶

The WFP estimates that 50% of their programming will be delivered as cash-based transfers by 2020. The organization estimates that the blockchain-based solution will reduce overhead transaction costs from 3.5 percent to 1 percent or less, saving millions of dollars.¹⁴⁷

Digital identity and electronic transfers of value are two areas where cash programming has benefitted from advances in this area. Irish start-up Aid:Tech¹⁴⁸ emphasizes the use of digital identity as an enhancement to voucher delivery, touting the ability to increase transparency, accountability, and efficiency. In December 2015 Aid:Tech piloted a program in Lebanon aimed at Syrian refugees. In the pilot, 100 beneficiaries were given digital debit cards loaded with \$20. The cards were only accepted at the camp store. While the trial was very small in scale, the results were promising: All cards were redeemed and 20 attempts at fraud were prevented. Aid:Tech's partner, the Irish Red Cross, was able to monitor the transactions in real time.¹⁴⁹

Refugee situations present problems where DLT solutions can be applied to some critical tasks. Digital identity systems, cash programming, and aid delivery could be enhanced through selective use of DLT. BitNation embarked on an ambitious program in this area. Named the Bitnation Refugee Emergency Response, the program sought to deliver a variety of DLT-enabled services to beneficiaries during the European refugee crisis of 2015. Services included a temporary digital I.D. and a Bitcoin Visa debit card.¹⁵⁰ Little information exists on the outcomes of the experiment. While the initiative appears to have little success, one has to wonder if this is at least part due to the fact that the initiative was created in reaction to the crisis, rather than beforehand.¹⁵¹

Cross-Border Cash Transfers

For a large multinational organization, an ability to quickly and cheaply move value across borders, and across currencies, would be a significant boon. According to one report, the settlement times for cross-border payments can take up to five days for even common currency pairings, with limited clarity as to the final costs and settlement timing. DLT solutions can enable asset movement in seconds (or minutes) and at greatly reduced costs, but challenges remain. Among the biggest issues to be solved are maintenance of local pools of liquidity, settlement with market makers, and compliance with local law.

3.4 Monitoring & Reporting

INGOs rarely provide donors with information relating to the ROI of particular projects, or the actual final use of funds that were given by the donor. The practical difficulties that make high levels of transparency difficult also create obstacles for cultivating trust, which can make it more challenging to raise donations. DLT has the potential to be helpful in building transparency and trust by providing enhanced traceability of funds.¹⁵²

¹⁴⁶ See, <http://www.coindesk.com/the-united-nations-wants-to-accept-ethereum-and-bitcoin-and-soon/>

¹⁴⁷ See, <http://innovation.wfp.org/project/building-blocks>

¹⁴⁸ See, <https://aid.technology/>

¹⁴⁹ See, <https://aid.technology/lebanon/>

¹⁵⁰ See, <https://refugees.bitnation.co/>

¹⁵¹ See, <https://venturebeat.com/2016/12/11/blockchain-and-humanitarian-causes-helping-those-who-need-it-most/>

¹⁵² See, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

“We’re exploring the use of a blockchain to manage the distribution of grants. Monitoring and controlling the use of grants is incredibly complex. A blockchain, accessible to all the parties involved, might be a better way of solving that problem... Think about ... the Department for International Development tracking money all the way to the aid organization spending the money in country..”

– Matt Hancock, UK Minister for the Cabinet Office

Implementation of DLT could make the data set associated with relief efforts easier to monitor and audit. Organizations who wish to reduce the burden of reporting while also increasing transparency may want to consider reporting financial transactions to a distributed ledger which is then shared with the parties responsible for monitoring. The monitoring party can see the data at any point in the process, thereby opening up the possibility to reduce the need for annual reporting, and perhaps even auditing. David Yermack of the NYU Stern School of Business describes how this could occur: “The company’s entire ledger would then be visible immediately to any shareholder, lender, creditor, or other interested party. Anyone could aggregate the firm’s transactions into the form of an income statement and balance sheet at any time...”¹⁵³

The potential DLT holds for improving transparency in humanitarian aid has not been lost on Jack Ma, Founder and CEO of Alibaba. Through the Alibaba subsidiary Ant Financial, a private, proof of work blockchain has been launched for the purpose of tracking charitable donations made through the AliPay platform.¹⁵⁴ The system is called AntLove, and at the end of 2015, it had connected 450 million users with more than 1,000 charities and was tracking more than 600 million yuan (~ \$86.8 million).¹⁵⁵ Using the system, donors are able to track transaction histories and understand better where and how their money is being used. In April of 2017, Alibaba announced expansion of the program to involve more donor organizations, charity groups, and media.¹⁵⁶

Digital currencies take transparency one step further, allowing donations to be tracked all the way from the donor to the beneficiary. While traditional currencies are fungible, this is not true for digital currencies or digitized assets. Each unit is unique and identifiable and, as a result, remains traceable throughout their lifespan, in a way that would be impossible for traditional currencies.

In the case of restricted funds, a donation earmarked for a particular purpose could be traced from the donor to the beneficiary, and each step along the way.¹⁵⁷ A DLT solution to

A Crisis in Confidence

Several recent reports indicate a trend towards lack of faith in the integrity of charities and how they use the donations they receive.

One study, from UK Fundraising, found that trust in charities has fallen from 6.7 (out of 10) in 2014 to 5.7 in 2016. The main reasons cited for this decline were distrust in how charities spend their donations, a lack of knowledge among the public about where their donations go, and media coverage critical of charity practices.

Moreover, a 2013 survey by New Philanthropy Capital revealed that donors found it hard to understand where their money goes and whether the charities they support make a difference. In that same survey, donors giving over £1.7bn said that they might be willing to switch their donations to charities that did a better job in the areas they care about.

¹⁵³ See, Yermak, D. (2015) *Corporate Governance and Blockchains*, NBER Working Paper 21802, Cambridge, MA: National Bureau of Economic Research

¹⁵⁴ AliPay is the largest online payment platform in the PRC and claims more than 400 million registered users (as of Oct. 2016). See, <http://expandedramblings.com/index.php/alipay-statistics/>

¹⁵⁵ See, <https://www.bloomberg.com/news/articles/2016-07-31/jack-ma-takes-on-murky-china-charities-in-first-blockchain-foray>

¹⁵⁶ See, <http://www.scmp.com/tech/china-tech/article/2086449/alibaba-affiliate-ant-financial-accelerate-blockchain-initiatives>

the issue of tracking restricted funds would increase transparency and might give donors greater confidence and encourage them to donate more.¹⁵⁸

The BitGive Foundation¹⁵⁹ has launched an initiative called GiveTrack, which they describe as a “Bitcoin charity 2.0 initiative.”¹⁶⁰ GiveTrack is designed to create a new standard of transparency in charity giving. As they describe it, the system will “allow donors and the public to trace nonprofit transactions on a public platform in real time to see how funds are spent, ensure they reach their final destination, and track the results generated from contributions.”¹⁶¹

The Water Project¹⁶² takes a similar approach, and is probably the organization most leveraging the transparency offered by Bitcoin and the blockchain. The project emphasizes transparency, with donors being able to trace their donation all the way to the final beneficiaries. While the impact of the project has been limited, the model they have piloted is significant, showing us how the future of charitable donations may evolve.

¹⁵⁷ Implementation of such a system could obviate the need for organizations like Give Directly, whose primary purpose is to give directly to individuals in need and track using electronic payment techniques. See, <https://www.givedirectly.org>

¹⁵⁸ The downside being that such a system may eventually lead to donors putting more restrictive conditions on donations, robbing organizations of much needed spending flexibility.

¹⁵⁹ See, <http://bitgivefoundation.org/>

¹⁶⁰ See, <http://bitgivefoundation.org/bitcoin-charity-2-0-initiative/>

¹⁶¹ See, *Ibid*.

¹⁶² See, <https://thewaterproject.org/>

4. Challenges to Adoption & Implementation

4.1 Governance

Regardless of how decentralized and distributed it is, a DLT still requires an agreed governance framework by which the participants operate. In addition to a consistent set of rules, a DLT needs a network administrator that is empowered to monitor, configure, and control the network as needed to maintain network integrity and protect the data.

Key issues include:

- Permissions and access management
- Rule setting
- Oversight
- Monitoring
- Validation and fraud detection
- Patch management
- Membership management
- Encryption and identity management
- Business continuity planning

Public DLT structures face the most difficulty in regards to governance. As we have seen with the highly decentralized Bitcoin community, building consensus and implementing changes to process and rules can be extremely challenging.¹⁶³

4.2 Operational Risks

DLTs have an unusual operational risk profile, flowing from the nature of the technology and to the fact that many systems lack a central authority to actively manage, administer, and control the operations. The risks are not insignificant and do require awareness, monitoring, and management.

¹⁶³ See e.g., The ongoing block size debate.

Notable risks include:

Data Storage & Retrieval

Distributed ledgers rarely store the underlying data, using instead hashes to represent the data. Accordingly, any DLT system needs to integrate with a robust data storage and retrieval system. The extent to which that integration is executed well impacts directly the usability and integrity of the DLT solution.

Network Problems

The backbone of any DLT is a network of nodes. In cases where there is a delay in transmission within the network, there is a potential for nodes to fall out of synch; at best, decreasing network efficiencies and at worst, leading to disputes over the state of the ledger. Network delays may be purely due to technical issues, or may be due to a malicious actor.¹⁶⁴ In either event, the greater the delay and disruption, the greater the likelihood for problems.

Malicious Nodes

In both public and private systems, there is potential for malicious nodes to inject problems into a DLT network. While most DLT consensus algorithms are designed to detect and exclude malicious nodes, the situation is more difficult to manage in open systems dependent on sometimes pseudonymous miners.¹⁶⁵

Identity Theft

Digital signatures are frequently used by DLT systems. In any case where digital signatures are relied upon, the burden is on the parties who are associated with those signatures to protect them. If an actor fails to take adequate precautions and their identity is stolen, the thief may well be able to manipulate the assets belonging to the legitimate owner. In a permissioned system, identity theft may also mean that an unauthorised person is able to gain access to the permissioned network and the data it contains.

Mis-use

Typically, transactions embedded in blocks are hashed, hiding their contents from casual observers. In cases where multiple actors are writing to the ledger, there exists the possibility to one or more of the actors is using the system for illegal or unethical purposes. Given that the data is hashed, it is difficult for other participants to gain insight into the legality of the transactions. Such potential is yet another reason closed systems are preferred in highly regulated industries, such as banking and finance.

4.3 Compatibility & Interoperability

As DLT networks find wider adoption, and the applications built on top of them diversify, compatibility and interoperability become significant issues. Currently few of the various blockchains have been built with an eye towards compatibility with competing systems. Given that many of the DLT projects presently under development are being tailored to narrow uses, and given the absence of accepted standards and best

¹⁶⁴ A distributed denial of service attacks (DDoS) is one foreseeable threat. While such an attack would be difficult to execute against a large distributed network, a smaller network could be overwhelmed, leading to slow downs in performance or temporary failure of the DLT network.

¹⁶⁵ In unpermissioned proof of work systems in particular, there exists the possibility that a group of dishonest miners can grab control of the blockchain; this is typically referred to as the 51% problem.

practices, the problem is likely to get worse before it gets better.

At present, a need for interoperability is most commonly dealt with through the use of a sidechain. A sidechain is a separate blockchain that runs in parallel to another blockchain, allowing data or assets to be moved back and forth between the two chains. Pegged sidechains suffer from a number of limitations that make scaling a solution impractical; they do not offer a long term solution to the problem of compatibility.

"One blockchain isn't going to do everything; we're going to have many blockchains."

- Marley Gray (Microsoft)

One of the most promising developments in this area is the birth of the Interledger Protocol. The Interledger Protocol¹⁶⁶ is an attempt to set out a standardized methodology for blockchains to talk to each other. The project claims: "Interledger is an open suite of protocols for connecting ledgers of all types: from digital wallets and national payment systems to blockchains and beyond."¹⁶⁷

The Interledger Protocol is not itself a ledger, as it does not seek consensus toward any state. Rather it provides a top-layer cryptographic escrow system that allows funds to move between ledgers with the help of intermediaries it calls "connectors".¹⁶⁸ The protocol may also help enable and thereby complement, sidechains, allowing sidechains to tie back into the primary blockchain easily. Though Interledger seems to hold the potential to do more, at this time the system is primarily about getting payments systems to talk to each other.

4.4 Risk Management & Regulatory Compliance

Any new technology brings with it a set of risks, and DLT is no different. While operating a DLT system in a permissioned configuration is an effective way to mitigate many of the security and scalability risks outlined above, other issues remain.

- Personal data privacy issues need to be addressed in any system where information concerning individuals is being stored. Compliance with data protection principles and with the individuals' right to correct data are both likely to be issues.
- In situations where a DLT operates across national boundaries,¹⁶⁹ issues such as cross-border data flow, legal enforceability, dispute resolution, discovery, and extraterritorial reach will need to be considered in the creation of the governance structure applied to the DLT.

While a comprehensive assay of legal and regulatory issues is beyond the scope of this paper, the potential issues are likely to be not insignificant and therefore will merit further study and consideration as part of any decision to adopt DLT.

¹⁶⁶ See, <https://interledger.org>

¹⁶⁷ See, <https://interledger.org/why-interledger.html>

¹⁶⁸ See, <http://www.coindesk.com/ripple-interledger-connect-bank-blockchain/>

¹⁶⁹ A situation possibly further complicated where nodes are operated in different jurisdictions.

5. Final Thoughts

5.1 On Timing

DLT is sometimes criticized as being a solution in search of a problem, but it may be the case that expecting a massively popular application that proves the importance of DLT is looking at this the wrong way. It may be that DLT's value will be felt in a larger number of less radical applications, each of which has small value but leads to a significant total. Vitalik Buterin, founder of Ethereum, notes: "The days of easy gains are over. Now is the time for a much hard(er) and longer slog of looking into the real world and seeing (if) the technologies we have built can actually benefit the world. During this stage, we will likely discover that at some point we will hit an inflection point, where most instances of 'blockchain for X' will be made not by blockchain enthusiasts looking for something useful to do, coming upon X, and trying to do it, but rather by X enthusiasts who look at blockchains and realize they are a fairly useful tool for doing some part of X."¹⁷⁰

At this stage in the evolution of this technology, we have already seen very significant investment of both time and resources by a wide range of industry players. Some commentators are speculating that 2017 is a make or break year and, that in the absence of demonstrable real-world implementations, that the technology risks crumbling under the weight of unfulfilled promise.¹⁷¹ While such a prediction appears overly dramatic, the question of the maturity of the technology is considerable.

"Blockchain is challenging industry players to fundamentally reimagine their data sharing processes. There is no turning back."

– Accenture, "Banking on Blockchain" (2017)

The overwhelming optimism that buoyed the blockchain market just a year ago has cooled somewhat as progress on practical solutions has been slower than expected. At the recent DTCC Fintech Symposium, the audience was asked for their predictions of how long it would take for DLT to hit the mainstream. Attendees were also asked about their perceptions of various risks. The previous year, the attendees had been asked the same questions.¹⁷² The responses are shown in the table, below. Expectations shifted dramatically. Where 32% of the people surveyed the previous year felt DLT solutions would be adopted by industry in 6 to 12 months, that number dropped to 3.9% in this year's survey.

¹⁷⁰ See, <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/>

¹⁷¹ See e.g., <http://www.coindesk.com/wait-see-do-die-experts-slow-blockchain-dlt-adoption-2017/>

¹⁷² As shown in the column headers, the 2016 conference had a different name: "Blockchain Symposium."

Question / Answer	2016 Blockchain Symposium	2017 Fintech Symposium
1) What aspects of implementing blockchain technology do you believe present the greatest challenges?		
Data Privacy and Security	12%	13.5%
Scalability and capabilities of the technology itself	21%	18.9%
Business case and cost of integration	32%	33.8%
Interoperability	n/a (answer wasn't offered)	20.3%
Legal and regulatory requirements	12%	10.8%
Other	4%	2.7%
2) When will a production ready distributed ledger solution be adopted by the industry?		
6 months to a year	32%	3.9%
1-2 years	24%	39.5%
3-4 years	16%	44.7%
5-6 years	11%	5.3%
More than 6 years	10%	6.6%

Source: CoinDesk.com

The question of when DLT will reach a practical level of maturity is not easily answered. Even the opinions of the experts currently testing the technology range widely: Maersk, currently trialing a supply chain management system with IBM, predicts it may take five or even ten years to get all the players involved in its system online and connected. In contrast, Walmart, who is also involved in a trial using IBM's tech, says it can be put together "in a few years."¹⁷³ These widely ranging predictions no doubt reflect in part the scale and complexity of the various initiatives under consideration, but they also show a clear shift in expectations – a shift towards more conservative estimates. The DTCC survey, above, may be the more reasonable middle ground, with 84.2% of the respondents estimating that a production ready DLT will be adopted by industry in one to four years.

5.2 On Use Cases

Numerous proofs of concept are currently in progress in various industries. In the relief and development sector, however, movement has been slower. Aside from the UN WFP's Building Blocks program, there are few examples to point to at this date. That said, there exists potential for DLT to be applied to multiple business problems confronting relief and development. Among the areas with the most potential are:

- **Financial inclusion**

Leveraging DLT for the benefit of the unbanked represents some of the most exciting progress in the field of financial inclusion in recent years. Micro-finance and micro-insurance are related areas that also show potential for the sector and merit further development.

¹⁷³ See, https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html?_r=0

- **Cash programming and delivery of social welfare**

The WFP's Building Blocks program provides one of the few proven use cases in this sector. The scaling of that program is being watched closely and is likely to inspire other similar efforts.

- **Better beneficiary ID and onboarding**

DLT, coupled with digital identity schemas, has the potential to bring a number of benefits to relief and development. Once a beneficiary's identity is established, the verified identity can be shared with other organizations in the network, avoiding the need to repeat the full identification and verification process, thus speeding up and increasing efficiency in the onboarding process.

- **Reduced beneficiary fraud**

Digital identity schemas can also help decrease fraud. Exactly what is delivered, and to whom, could be logged in a shared ledger. The system would refuse multiple claims for the same aid, as you would know what had already been delivered and to whom. Smart contracts could also be used to pay out only when specific conditions are met.

- **Tracking of support to beneficiaries from multiple sources**

A shared ledger among multiple agencies could generate a snapshot of lifetime aid delivered to specific beneficiaries, enabling better assessment of effectiveness and outcomes. Again, a reliable identity schema is critical for success.

- **Land titling**

The ability for the disenfranchised to establish title to hereditary lands can unlock hidden capital and transform the lives of many currently living in poverty.

- **Enhanced transparency of donations**

Though increased transparency will create challenges for many agencies, the opportunity DLT presents to build trust among donors is significant.

- **Grant management and organizational governance**

Use of smart contracts and a DLT registry for assets and transactions can reduce costs, improve transparency, and lessen the burden of auditing.

The list, above, is not meant to be comprehensive; additional use cases will emerge as the sector starts to embrace DLT as an enabling technology. Moreover, other areas where DLT is likely to benefit relief and development, for example, asset management, remittances, or cross-border transfers, are already being explored by the fintech world; in those areas, applications are likely to be developed elsewhere and leveraged by our sector. Regardless of whether the apps are built within the sector, or elsewhere, the deployments in this sector need to reflect the distinct characteristics and data priorities of our work with beneficiaries and oversight agencies.

Deploying DLT arrangements should be considered when at least some of the following conditions are present:

- There is a desire for increased resiliency through distributed data management
- There is a need for increased transparency in recordkeeping
- There is a need to track asset ownership between multiple actors and over time
- Complexity can be reduced
- Processing speed and availability of assets and funds can be improved
- The need for reconciliation can be reduced
- A record, or proof of transaction, is required
- There is important information that needs to be communicated and stored in a highly secure manner, and this is currently being done by way of a largely manual, labor-intensive or paper-based process.

5.3 On an Approach

DLT is likely to impact companies that specialize in providing trust in a similar fashion to how the internet impacted media companies – by introducing major disruption to their markets. Banks, lawyers, and financial services will be the first ones to feel the impact, but it won't stop there. To the extent to which relief and development organizations provide trust – trust that the funds were used for the stated purpose, trust that the right beneficiaries received the aid, trust that the work was actually done on time and as described – DLT will disrupt the sector. Though the extent to which DLT impacts the architecture of humanitarian actors has yet to be defined, the technology carries significant potential.

While the issues, above, are important, the larger question is how to frame an approach to DLT. Don't ask *"what business problem will DLT solve?"* DLT is not the end solution – it is a methodology for implementing a solution. Accordingly, it is more appropriate to ask, *"where is the inefficiency that needs to be solved?"* or *"how would a decentralized approach affect our processes and enable what was not practical before?"*

At present, the most obvious use of DLT is to enhance existing architecture, perhaps by supplanting old mechanisms. While the other option, that is, the replacement of entire business processes by DLT, is a possibility, it is less likely due to a variety of practical factors, including cost and disruption.

One caveat worth noting: If NGOs merely try to retrofit DLT into their existing infrastructure, they will potentially miss the larger opportunity. Existing processes reflect the centralised structure of most NGOs, and were never designed for exploiting the sort of opportunities DLT brings, that is: Radical transparency, automated execution of contract terms, and open collaboration with other agencies. To truly maximize the benefit of DLT, relief and development agencies need to think bigger, and reimagine their

"If you think about the way authentication and identification is done, the way you onboard customers, the way you share records, all of this is done through siloed, decades-old channels and processes. And here you have a technology that basically says you no longer need a middleman... You're basically saying, we're going to change the way the economic models that have grown up for the last several centuries operate. As a result, we're going to change the way society operates as well."

- David Furlonger, Gartner

processes so that the beneficiary is the central point of the data systems, and the ability to collaborate across the sector is fundamental. The discussion, arguably, needs to occur at the sector level, with a fresh look at the relationship between processes, beneficiaries, and organisations and how the use of DLT will allow agencies to improve efficiency and reduce costs across the sector.

While early DLT work in humanitarian and relief has been focused on solving specific problems, or optimizing existing processes, there is an opportunity to address how DLT can be used to address sector-wide challenges and opportunities. DLTs are intrinsically low-cost and can help avoid duplication and inefficiencies in control and coordination by enabling a common open ledger that can operate at an industry level. Such an approach would reduce systemic costs involved in processes like cross-checking individually held ledgers and databases.¹⁷⁴

“Innovation can also occur within business models, and often legitimize new relationships within an industry to create ‘cooptation’, where firms both co-operate and compete.”

– UK Government Chief Scientific Adviser (2016)

As Deloitte observes, “There are considerable opportunities for organisations that adopt blockchain technology internally...Perhaps the most significant opportunity, though, comes from blockchains that link currently disparate parts of one enterprise together *or even many different organisations from within the same sector.*”¹⁷⁵ (emphasis added)

The relief and development sector could benefit from an industry-specific DLT architecture. Given that the industry is composed of a variety of independent organisations, who work under the scrutiny of agencies dedicated to oversight, and for the benefit of third-party beneficiaries, the information sharing dynamic in relief and development is not dissimilar to that in banking and finance, where competitors work under the eye of regulatory agencies for the benefit of customers. In both cases as well, paperwork requirements are significant and auditability is a major concern. Just as banks must know their customers, NGOs are increasingly under pressure to know the identities of their beneficiaries and assure that aid winds up in the hands of the intended beneficiaries. And, just as in banking and finance, beneficiaries often have contact with other organisations in our sector.

In such an environment, a distributed ledger, shared among the players in the sector, has the potential to deliver significant benefits to the sector as a whole, as well as to the individual players. A DLT that allows different humanitarian agencies to collect data on the same network would enable agencies to reduce costs related to information sharing while still maintaining the integrity and, where needed, the privacy of the data.¹⁷⁶

A DLT Ecosystem

While the present development dynamic is typified by siloed efforts, the time will eventually come when standards of interoperability reach the point that systems can begin talking to each other easily. The real potential of the technology, in terms of operational efficiencies, opens up with the birth of a DLT ecosystem -- when the digital identity frameworks talk to the various data systems, as well as the payment mechanisms, under the guidance of a layer of smart contracts. This potential has clearly not been missed by Estonia and the UAE, who are already moving aggressively to achieve this ecosystem.

¹⁷⁴ See, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

¹⁷⁵ See, <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf>

¹⁷⁶ At least one author has observed that a blockchain-based data-sharing system could be built to complement the existing OCHA Humanitarian Data Exchange. See, Ko and Verity, “Blockchain for the Humanitarian Sector: Future Opportunities, ” (2016).

Creating a distributed ledger among a group of collaborating organisations brings a number of advantages:

- Improved network availability, reliability and maintainability
- Increased speed of data exchanges, which can reduce backlogs and overall costs
- Improved auditability
- Increased efficiency by standardising data formats and improving interoperability and process integrity
- Reduced risk of fraud
- Improved data sharing
- Ability to share costs among participants

The time is right for the relief and development sector to form a consortium or, at the very least, a working group, with the goal of examining how DLT can be deployed in the sector. The group should examine the opportunities, consider the infrastructure needs, and set a goal to define standards of interoperability and best practices. The group should also look at strategic partnerships and consider how costs can be shared among players.

Lacking a consortium focused on developing this technology in a manner appropriate to our sector, we are at risk of falling into the old pattern of individual, siloed development efforts, an approach that is proven to be both expensive and inefficient. While some individual organizations will no doubt continue to develop solutions in isolation, if that approach becomes dominant, the sector runs the risk of missing the bigger opportunity, that is, the ability to share data, reduce the burden of regulatory oversight and audit, and improve our view of beneficiaries and the impact of our work. Small players currently lead in exploring DLT; major players need to get on board and bring their considerable resources to bear.

APPENDIX A: Noteworthy Platforms

While Bitcoin may be the best-known blockchain, there exist a number of other well-established alternatives, with yet more under development. Inspired by Satoshi's original concepts, and armed with the knowledge of the shortcomings of the Bitcoin blockchain in actual implementation, a number of alternative DLT schemas developed. The innovative variations relate to three primary areas:

1. Consensus mechanisms,
2. Access to the data in the ledger, and
3. Anonymity.

In this section we look at five of the leading names.

The Original: Satoshi's Blockchain

The concept of a blockchain was first promulgated by Satoshi Nakamoto in a white paper released in November, 2008. That white paper was entitled "Bitcoin: A Peer-to-Peer Electronic Cash System"¹⁷⁷ and set forth the idea of a digital currency system to be called Bitcoin. The paper described a digital currency that used a peer-to-peer distributed ledger to keep track of the ownership and transfer of Bitcoin. As Satoshi described it, "transactions are recorded in blocks that are then chained together to provide a continuous record of transactions." It from that description that we derive the term "blockchain."

The original Bitcoin blockchain was built for one purpose: To track the ownership and transfer of the digital currency Bitcoin. Subsequently, as people have begun to appreciate the potential of the peer-to-peer distributed ledger at the heart of the blockchain, we have seen multiple attempts to retrofit the Bitcoin blockchain with enhancements, or ancillary structures, that expand the functionality.

Bitcoin Blockchain Characteristics

Participation of untrusted peers	Yes
Primary application	Payments
Support for Smart Contracts	Not built for this purpose, but suitable for payment contracts.
Database Structure	Blockchain
Consensus Mechanism	SHA-256 Hash + Proof of Work
Associated cryptocurrency	Bitcoin
Transparency	Accessible to all
Turing Complete?¹⁷⁸	No

¹⁷⁷ See, <https://bitcoin.org/bitcoin.pdf>

¹⁷⁸ "Turing Complete" refers to system that can solve computational problems at a level at least equivalent to a single tape Turing machine. Put in other words, it is a system that is able to run algorithms and preform programmed tasks. A system that is not Turing complete could not, for example, run Smart Contracts.

The Ripple Protocol¹⁷⁹

Ripple is focused on the financial sector, offering a protocol to facilitate real-time cross-border payments and easy settlements. Ripple functions on the back of a private network of trusted participants and does not employ a blockchain structure. The Ripple Protocol, as it is known, is a distributed open source network protocol that employs a consensus mechanism to enable transactions among known participants. The system also has a native cryptocurrency, known as XRP.¹⁸⁰ Among the financial institutions using the Ripple Protocol are USB, Santander, Westpac, Commonwealth Bank of Australia, ANZ and Standard Chartered.¹⁸¹

Ripple Protocol Characteristics

Participation of untrusted peers	No
Primary application	Settlement
Support for Smart Contracts	None¹⁸²
Database Structure	Non-blockchain
Consensus Mechanism	Byzantine Altruistic Rational (BAR)
Associated cryptocurrency	Ripple (XRP)
Transparency	Access limited by permissions.
Turing Complete?	No

Ethereum¹⁸³

Ethereum is an open source public blockchain designed to function as a platform for various computing applications and smart contracts. Ethereum came into the market significantly later than Bitcoin,¹⁸⁴ and took a different approach. Though Ethereum uses a public blockchain in the fashion of Bitcoin,¹⁸⁵ the developers built a flexible logic layer that make the blockchain suitable for more than just payments and a digital currency.

The developer community, and investors, embraced Ethereum quickly. As of March 2017, Ether, the digital currency associated with Ethereum, was the second-largest cryptocurrency by market cap, lagging behind only Bitcoin. Enterprise interest in the use of the Ethereum blockchain is also high, with demos of Ethereum projects seen from JP Morgan, Microsoft and Deloitte.

¹⁷⁹ See, <https://ripple.com/>

¹⁸⁰ At the time of writing, XRP was the third largest cryptocurrency by market cap, behind Bitcoin and Ethereum.

¹⁸¹ See, <http://bankinnovation.net/2016/09/ripple-raises-55m-as-client-list-grows-to-15-of-top-global-banks/>

¹⁸² Ripple Labs released a smart contracts platform known as Codius, however, it appears to have ceased development. See, <https://codius.org>

¹⁸³ See, <https://www.ethereum.org/>

¹⁸⁴ Ethereum was launched on 30 July 2015.

¹⁸⁵ In a bit to improve security and enhance scalability, Ethereum is exploring moving away from a Bitcoin-type system dependent on miners (i.e., proof of work), to a proof of stake mechanism. See, <https://www.bloomberg.com/news/articles/2017-02-28/bitcoin-s-top-rival-is-up-90-and-readying-its-next-big-move>

Ethereum Blockchain Characteristics

Participation of untrusted peers	Yes
Primary application	Payments
Support for Smart Contracts	Suitable for a variety of applications.
Database Structure	Blockchain
Consensus Mechanism	EtHash + Proof of Work
Associated cryptocurrency	Ether (ETH)
Transparency	Accessible to all
Turing Complete? (language)	Yes (Solidity)

Corda¹⁸⁶

Corda is a distributed ledger platform designed for the recording and automation of legal agreements between identifiable parties. Although heavily influenced by the needs of the finance industry, Corda is flexible enough to cater to a wide variety of applications. Corda restricts access to data to only those explicitly entitled to it and financial agreements are designed to be enforceable and firmly rooted in the law.¹⁸⁷

Corda was originally developed by the consortium R3.¹⁸⁸ The code for Corda was open-sourced and added to the Hyperledger Project in November of 2016.

Initial reaction has been mixed. The architecture of Corda is quite different from other systems, leading some commentators to characterize it, not as a blockchain or DLT, but rather as “a shared ledger”, or even “a messaging protocol.”¹⁸⁹ Corda uses a trusted peer system that allows the participants in the transaction to validate the transaction, and thereby maintain a high level of privacy. All transactions in the system are governed by one or more smart contracts that specify which operations are allowed and who can conduct them. The system also provides for limited access to the data via regulatory or observer nodes.

Unlike Bitcoin and Ethereum, there is no cryptocurrency associated with Corda.

¹⁸⁶ See, <https://www.corda.net/>

¹⁸⁷ See, <http://www.r3cev.com/blog/2017/2/24/when-is-a-blockchain-not-a-blockchain>

¹⁸⁸ See, *supra*.

¹⁸⁹ See, <http://www.gtreview.com/magazine/volume-15issue-3/r3s-corda-uncovered-not-blockchain/>

Corda Platform Characteristics

Participation of untrusted peers	No
Primary application	Financial applications
Support for Smart Contracts	Suitable for a variety of applications.
Database Structure	Non-Blockchain
Consensus Mechanism	Mix of approaches
Associated cryptocurrency	None
Transparency	Access limited by permissions
Turing Complete? (language)	Yes (Java and others)

Hyperledger Fabric¹⁹⁰

The Hyperledger Project is currently incubating a number of initiatives.¹⁹¹ The Fabric project is the first to launch as an active product; it aims to provide a plug and play modular architecture that will allow businesses to spin up DLT-backed applications quickly and with lower risk. Using Fabric, participants in the blockchain network can create channels in which they are able to transact with others, and specify varying degrees of access and privileges. IBM is the first major player to offer solutions using Fabric.¹⁹²

Hyperledger is quite active and there are substantial proofs of concept with multiple partners in progress, including tests by Deutsche Borse, SWIFT, Post Savings Bank of China, DTCC and more.¹⁹³

Hyperledger Fabric Characteristics

Participation of untrusted peers	No
Primary application	Various
Support for Smart Contracts	Suitable for a variety of applications.
Database Structure	Blockchain
Consensus Mechanism	Practical Byzantine Fault-Tolerant (PBFT) and others
Associated cryptocurrency	None
Transparency	Access limited by permissions
Turing Complete? (language)	Yes (Golang and Java)

¹⁹⁰ See, <https://www.hyperledger.org/>

¹⁹¹ See, supra.

¹⁹² See, <http://www.coindesk.com/ibm-goes-live-first-commercial-blockchains/>

¹⁹³ See, https://www.hyperledger.org/industries/finance#poc_tracker

APPENDIX B: Solutions Providers

- **Amazon**

In May of 2016, it was announced that Amazon Web Services intended to partner with the Digital Currency Group¹⁹⁴ to offer blockchain as a service.¹⁹⁵ Since that announcement, however, there has been no further news, and the current Amazon Web Services site shows no sign of the product.¹⁹⁶

- **B3i¹⁹⁷**

The B3i project – short for the Blockchain Insurance Industry Initiative – was launched in October, 2016.¹⁹⁸ The project aims to provide a collaboration space for insurance industry players to experiment with DLT. Members include Allianz, Hannover, Liberty Mutual and other major players. The consortium is prioritizing development of a prototype platform for exchanging contracts, with the goal of spinning off a separate business entity by 2018.¹⁹⁹

- **Chain**

Chain provides permissions and private blockchain services for enterprises. One of the firm's distinctives is an emphasis on privacy. Chain's confidential assets scheme hides the transaction amount and account identity on the ledger. Chain partnered with Nasdaq on the Linq platform and in late 2016, they partnered with Visa to introduce an international B2B payment solution. Chain's open source DLT platform is also generating a significant amount of interest in the industry at the moment.

- **ChinaLedger Alliance²⁰⁰**

Wanxiang Blockchain Labs, a Shanghai-based nonprofit research institution, is to lead an alliance of 11 regional commodity exchanges, equity exchanges, and financial asset exchanges with the aim of creating an open source blockchain protocol that developers can further build upon in the future.²⁰¹ The consortium was announced in May of 2016, but there seems to have been little mention since the launch announcement.²⁰²

¹⁹⁴ See, <http://www.dcg.co>

¹⁹⁵ See, <http://www.forbes.com/sites/laurashin/2016/05/02/amazon-steps-up-blockchain-commitment-web-services-partners-with-digital-currency-group/#2cd846d9712e>

¹⁹⁶ There are, however, some third-party vendors who are offering support for blockchain applications via AWS. See e.g., <https://aws.amazon.com/marketplace/pp/B01BTB1EP8>

¹⁹⁷ See, http://www.swissre.com/reinsurance/insurers_and_reinsurers_launch_blockchain_initiative.html

¹⁹⁸ See, <http://www.coindesk.com/europe-insurance-blockchain-consortium/>

¹⁹⁹ See, <http://www.reuters.com/article/us-insurance-blockchain-swiss-re-idUSKBN15924K>

²⁰⁰ See, <http://www.chinaledger.com/>

²⁰¹ See, <https://bitcoinmagazine.com/articles/china-joins-the-blockchain-race-with-chinaledger-alliance-1462204569>

²⁰² Indeed, the group's Twitter account has been dormant since June, 2016. See, <https://twitter.com/chinaledger>

- **Deloitte**

In what came as a surprise move to many, Deloitte launched a BaaS product known as “Rubix.”²⁰³ Using the Rubix platform, clients can prototype, test, and build customized blockchain and smart contract applications. Rubix uses a private network infrastructure optimized for enterprise use.

- **Digital Asset**

Digital Asset is a blockchain software provider focused on distributed asset settlement. The company was founded by Blythe Masters, former General Manager of JP Morgan, and counts as its investors a number of major names from banking and finance. One of the company’s distinctives is the Global Synchronization Log (GSL), a potential solution to blockchain compatibility and interoperability.

- **Hyperledger**²⁰⁴

The Hyperledger Project was launched by the Linux Foundation in December of 2015. The stated purpose of the project was to collaborate on the development of an “an open platform that will satisfy a variety of use cases across multiple industries to streamline business processes.”²⁰⁵ The membership of the Hyperledger Project features over 100 major firms from a wide swath of industry, from finance, to supply chain, to software development, and beyond. R3 (see, above) is also a member.

Though Hyperledger bills itself as cross-sector, to date the focus has largely been on finance and healthcare related projects, with supply chain efforts evidently next in line.²⁰⁶ As of 15 March 2017, the following frameworks were under incubation at Hyperledger:²⁰⁷

- **Fabric:** “An implementation of blockchain technology that is intended as a foundation for developing blockchain applications or solutions. It offers a modular architecture allowing components, such as consensus and membership services, to be plug-and-play. It leverages container technology to host smart contracts

Blockchain as a Service (BaaS)

BaaS brings the Platform-as-a-Service (PaaS) concept to the world of DLT. Big players, such as Amazon, IBM and Microsoft, are able to leverage their cloud architecture and offer companies and individuals a way to quickly deploy DLT apps using a variety of pre-existing blockchain options.

For DLT applications that wish to run on private blockchains in particular, BaaS presents a desirable option. While public blockchains enjoy the benefit of a vast peer-to-peer (P2P) network of nodes and machines to perpetuate and reinforce the decentralized infrastructure, private blockchains require substantial manual development effort and back-end computing capacity to build and maintain a viable infrastructure. Thus, there is a market for BaaS vendors, who can host private blockchains and do the heavy lifting. Perhaps most importantly, the rise of BaaS means that the cost for creating innovative applications drops dramatically. New solutions can deploy fast, scale fast, and, when necessary, fail fast.

²⁰³ See, <http://rubixbydeloitte.com/>

²⁰⁴ See, <https://www.hyperledger.org/>

²⁰⁵ See, <https://www.hyperledger.org/announcements/2016/02/09/linux-foundations-hyperledger-project-announces-30-founding-members-and-code-proposals-to-advance-blockchain-technology>

²⁰⁶ See, <https://www.hyperledger.org/industries>

²⁰⁷ In addition, Since inception, code has been donated to the project from a number of sources. On 30 November, 2016, the Corda code (from R3) was also contributed to the Hyperledger project.

called “chaincode” that comprise the application logic of the system.”²⁰⁸

- **Iroha:** Inspired by Fabric, Iroha is designed to enable C++ developers to actively contribute to development of Hyperledger projects.
- **Sawtooth Lake:** A modular blockchain project originated by Intel. It features both permissioned and permissionless alternatives and is built on a relatively novel consensus algorithm known as Proof of Elapsed Time (PoET).

Hyperledger is also incubating a number of additional projects (or “modules”) and the list of projects bound to grow as members continue to submit new initiatives for consideration.²⁰⁹

- **IBM**

IBM has brought to market a blockchain as a service offering that leverages their existing cloud infrastructure.²¹⁰ The company is providing a BaaS product, along with developer support. IBM is also an active member of the Hyperledger Project, and has launched the first commercial application of Hyperledger’s Fabric codebase. The product is called “IBM Blockchain” and its first two major deployments were announced in March 2017.²¹¹

While IBM’s product offerings are similar to Microsoft’s in many regards, IBM is taking a more aggressive approach to blockchain technologies.²¹² In addition to the firm’s active support of the Hyperledger Project, IBM has also launched a series of blockchain incubators in seven different locations to help build and support the creation of blockchain-related startups.²¹³

- **Microsoft**

Microsoft moved into the blockchain space with the launch of the Azure Blockchain as a Service (BaaS) product. While Microsoft’s Azure BaaS primarily leverages the Ethereum blockchain, the system does provide several alternatives for access and consensus mechanisms.

- **R3 CEV²¹⁴**

R3 CEV (R3) is an industry-specific blockchain consortium focused on the finance industry. Founded in September of 2015, the initial membership included a number of major financial players, including Credit

²⁰⁸ See, Ibid.

²⁰⁹ At the time this was being written the first Ethereum-powered project had also been submitted to Hyperledger, but had yet to be formally accepted. If accepted, it will certainly spur continued interest in the use of Ethereum for enterprise apps. See, <http://www.coindesk.com/hyperledger-to-gain-first-ethereum-virtual-machine-with-monax-membership/>

²¹⁰ See, <https://www.ibm.com/blockchain/>

²¹¹ See, <http://www.coindesk.com/ibm-goes-live-first-commercial-blockchains/>

²¹² The NYTimes reports that more than 650 people are currently dedicated to blockchain tech at IBM. See, <https://mobile.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html>

²¹³ These projects are known as IBM Bluemix Garages. See, <http://seekingalpha.com/article/4003831-will-microsoft-ibm-blockchain-world>

²¹⁴ See, <http://www.r3cev.com/>

Suisse, UBS, Barclays, Goldman Sachs and JP Morgan. By 2017, the consortium had expanded to include more than 70 firms, primarily from the finance industry.²¹⁵

The consortium focuses their efforts on the development of an open source blockchain platform named Corda. The Corda blockchain has been developed with financial services in mind and features enhanced ability to handle complex transaction data and the ability to restrict access to that data.²¹⁶ The consortium has announced two large tests involving multiple institutions, but at this time the logical evolution of the platform remains unclear.

In addition to the Azure Blockchain product, Microsoft has released a middleware solution named Project Bletchley.²¹⁷ Project Bletchley is aimed at developers and closes some gaps in BaaS architecture. As Microsoft describes the purpose of Project Bletchley: “To supply enterprise grade services around identity, security, cryptography, scale, tooling, management, monitoring and reporting.”²¹⁸

- **Revolution 4**

In October, 2016, Overstock announced the intention to launch a new blockchain consortium that would be less expensive than the major players and allegedly open to wider membership. Overstock has not yet announced a launch timeline.²¹⁹

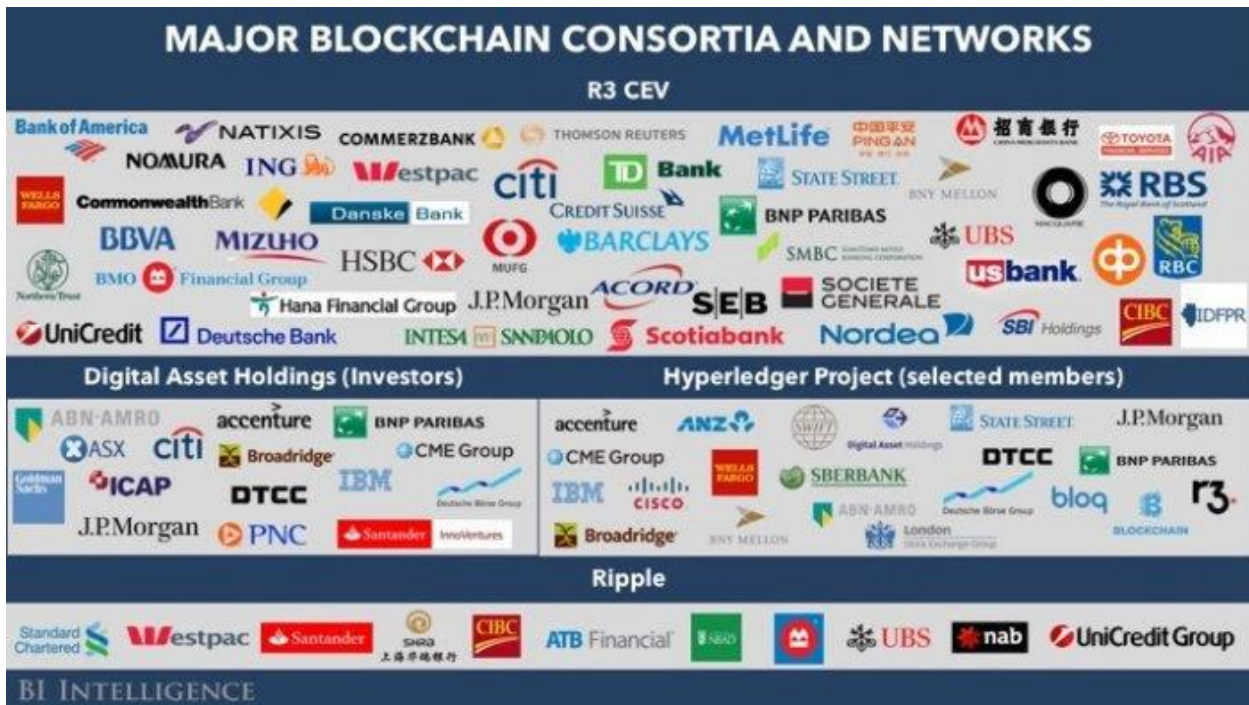
²¹⁵ Shortly before the release of this paper, it was announced that both Santander and Goldman Sachs, one of the founders of R3, have withdrawn from the consortium. Though the reasons for Santander's decision are unknown, Goldman-Sachs departure appears to be linked to a recent funding raising round and disagreement over control of the consortium. Another source cited Goldman Sachs' disapproval of the size of the consortium and the resulting difficulties in arriving at consensus. At the time of writing, rumors indicated that up to seven members of the consortium have yet to commit to the funding round.

²¹⁶ [https://en.wikipedia.org/wiki/R3_\(company\)](https://en.wikipedia.org/wiki/R3_(company))

²¹⁷ See, <https://azure.microsoft.com/en-us/blog/bletchley-blockchain/>

²¹⁸ See, <https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md#bletchley>

²¹⁹ See, <http://www.coindesk.com/no-r3-overstock-plots-blockchain-consortium-for-everyone-else/>



Source: Business Insider, April 2017

APPENDIX C: Standards Bodies

DLT is still largely devoid of widely agreed upon standards. Several organizations are currently involved in framing standards and best practices. Here's a look at the biggest players in this emerging area.

- **European Securities and Markets Authority (ESMA)²²⁰**

The European Union's market watchdog, ESMA, released a white paper on blockchain and distributed ledger technology in June of 2016.²²¹ The release was coupled with a call for feedback. The purpose: "The consultation will help ESMA to assess the opportunities and challenges posed by DLT from a regulatory standpoint and form an opinion on whether a specific regulatory response to the use of this technology in securities markets is needed."²²² Though the agency has yet to release a formal opinion on the subject, one spokesperson has stated that "the capacity of distributed ledger technologies to fit into the existing regulatory framework may limit its deployment."²²³

- **International Organization for Standardization (ISO)²²⁴**

In April of 2016, Australia put forth a proposal to the ISO, advocating for the promulgation of internal standards for blockchain technology.²²⁵ In September of 2016, the proposal was accepted by the ISO, and Australia Standards was named to lead the committee.²²⁶ At present, the Blockchain and Electronic Distributed Ledger Technology Committee has 16 participating countries and is just beginning their work; accordingly, the scope of the work is as yet unknown.²²⁷

- **International Securities Association for Institutional Trade Communication (ISITC)²²⁸**

ISITC has a history of successfully formulating and championing standards to formal standards bodies, like ISO.²²⁹ The organization formed the Blockchain DLT Working Group in order to: "...provide a platform for the securities industry players to educate, discuss and validate the emerging Blockchain (or Distributed Ledger) technologies and its role in securities processing."²³⁰ In July of 2016, ISITC took on the task of proposing standards for blockchain technology, in ten areas.²³¹ At present, the group is taking feedback from partners and industry players as part of their initial research into formulating recommendations.

²²⁰ See, <https://www.esma.europa.eu/>

²²¹ See, https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf

²²² See, <https://www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies>

²²³ See, <http://fortune.com/2016/06/02/eu-watchdog-looks-deeper-into-blockchain/>

²²⁴ See, <http://www.iso.org>

²²⁵ See, <http://www.standards.org.au/OurOrganisation/News/Documents/Media%20Release%20-%20International%20Blockchain%20Standard%20-%202014%20April%202016.pdf>

²²⁶ See, <http://www.standards.org.au/OurOrganisation/News/Documents/Australia%20to%20lead%20international%20blockchain%20standards%20committee.pdf>

²²⁷ See, http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=6266604

²²⁸ See, <http://www.isitc-europe.com/>

²²⁹ See, <http://www.isitc-europe.com/about-us>

²³⁰ See, <http://www.isitc-europe.com/working-groups/blockchain>

²³¹ See, <http://www.isitc-europe.com/files/documents/160705-ISITC-Website-Standards.pdf>

- **Object Management Group (OMG) Finance Domain Task Force**

The OMG has launched the Distributed Ledger Technology Working Group. The group has chosen to focus on standards related to smart contracts, but has yet to release any formal proposals.²³²

- **W3C²³³**

The World Wide Web Consortium (W3C) hosts a Blockchain Community Group.²³⁴ The Blockchain Community Group is an informal working group whose stated mission is “...to generate message format standards of Blockchain based on ISO20022 and to generate guidelines for usage. This group will study and evaluate new technologies related to blockchain, and use cases such as interbank communications.”²³⁵ Given the organization’s extensive track record promoting standards and best practices for the web, it is conceivable that this group will become at least an influencer in the blockchain ecosystem.

- **XBRL²³⁶**

XBRL is an open standard for international business reporting. It is managed by a non-profit consortium supported by more than 600 organizations. XBRL is currently partnering with ConsesSys to formulate standards for tokenization of assets on the blockchain.²³⁷

²³² See, http://www.omgwiki.org/OMG-FDTF/doku.php#fdtf_distributed_ledger_technology_dlt_working_group

²³³ See, <https://www.w3.org/>

²³⁴ See, <https://www.w3.org/community/about/>

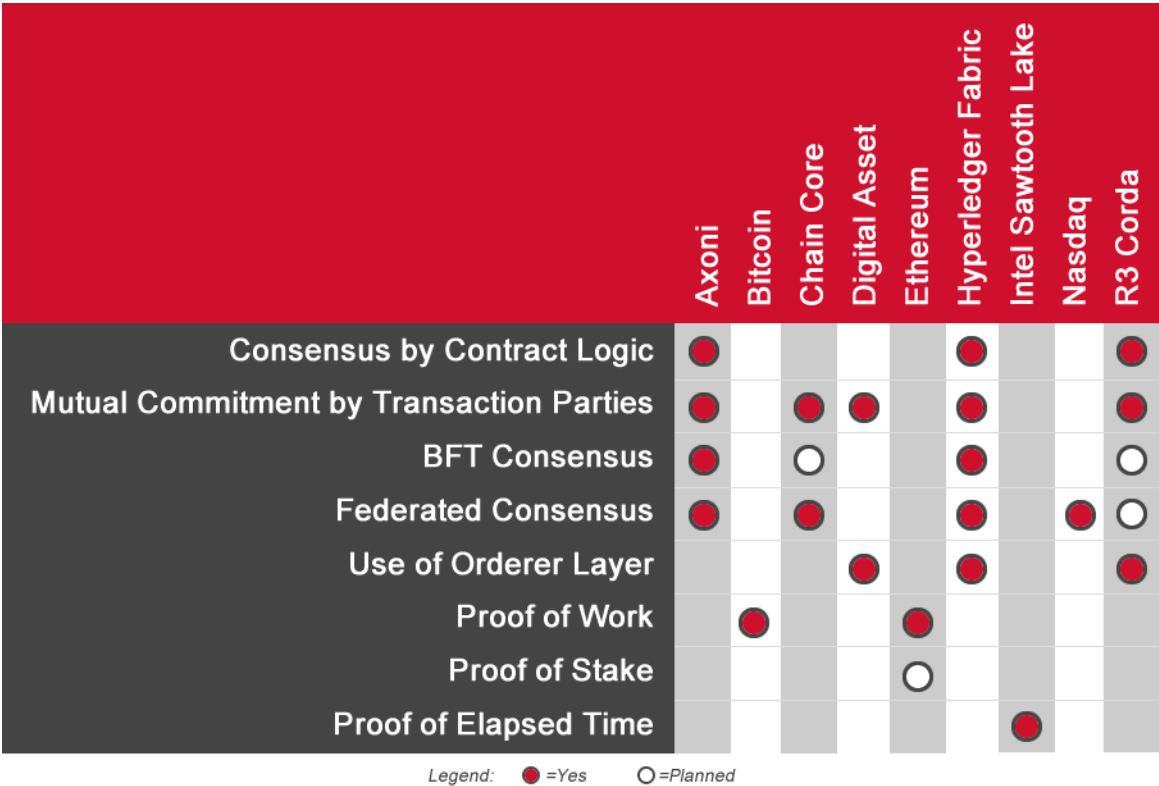
²³⁵ See, <https://www.w3.org/community/blockchain/>

²³⁶ See, <https://www.xbrl.org/>

²³⁷ See, <http://fintechranking.com/2016/12/20/consensus-looks-to-establish-blockchain-tokenization-standards/>

APPENDIX D: Consensus Methods

DLT implementations of consensus algorithms typically vary in terms of how their technical structures are designed to optimize performance, scalability, consistency, threat model, or failure model. The chart, below, shows the methods used by the various systems discussed in this paper.



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

CONTACT

RIC SHREVES

Manager | Internal Communications and Knowledge
Management

rshreves@mercycorps.org

About Mercy Corps

Mercy Corps is a leading global organization powered by the belief that a better world is possible. In disaster, in hardship, in more than 40 countries around the world, we partner to put bold solutions into action — helping people triumph over adversity and build stronger communities from within. Now, and for the future.



45 SW Ankeny Street
Portland, Oregon 97204
888.842.0842
mercycorps.org