How much does trust cost?
- Analysis of the consensus mechanism of distributed ledger technology and use-cases in securitization

By

Jennifer Hongbo Jiang

Bachelor of Economics in Statistics, 1994
M.B.A. McGill University, 1999

SUBMITTED TO THE MIT SLOAN SCHOOL OF MANAGEMENT IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN MANAGEMENT OF TECHNOLOGY
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2017

©2017 Jennifer Hongbo Jiang. All rights reserved.

The author hereby grants to MIT permission to reproduce
and to distribute publicly paper and electronic
copies of this thesis document in whole or in part
in any medium now known or hereafter created.

Signature redacted  MIT Sloan School of Management
May 12, 2017

Certified by:_________________________ Christian Catalini

Fred Kayne (1960) Career Development Professor of Entrepreneurship
Assistant Professor of Technological Innovation, MIT Sloan School of Management
Thesis Supervisor

Accepted by:_________________________ Johanna Hising DiFabio

Director, Sloan Fellows and EMBA Programs
How much does trust cost?
- Analysis of the consensus mechanism of distributed ledger technology and use-cases in securitization

By

Jennifer Hongbo Jiang

Submitted to MIT Sloan School of Management
on May 12, 2017 in Partial Fulfillment of the
requirements for the Degree of Master of Science in Management of Technology.

ABSTRACT

This paper analyzed how blockchain has achieved decentralized consensus, a remarkable innovation by: 1) validating transactions based on cryptograph technologies and implicit incentives; 2) extending blockchain networks based on a process of randomization. The success of emerging distributed ledger technology (DLT) reveals an intricate interplay of key factors among technology, economics, and rules. This paper discussed the broad spectrum of permissionless and permissioned DLTs and argued that the choice of DLT for each business case is a delicate balancing act for the needs of disintermediation, confidentiality, and scalability among other considerations. Smart contacts are the pre-agreed set of rules evaluated and executed by an automated system based on DLT. By digitalizing the physical business world, smart contracts combined with IoT or big data analytics can help make powerful business cases, and we illustrated the potential use-cases in financial securitization industry. Looking forward, a decentralized consensus model empowered by DLT may lead to a new dimension of organizational changes and foster more collaborative partnership within and beyond the financial services industry.

Thesis Supervisor: Christian Catalini
Title: Fred Kayne (1960) Career Development Professor of Entrepreneurship
Assistant Professor of Technological Innovation
List of Figures

Figure 1. Bitcoin price and total number in circulation as of Apr 3, 2017 ................................................................. 9
Figure 2. Momentum of interests in Blockchain ............................................................. 9
Figure 3. Venture capital in Bitcoin and blockchain ..................................................... 10
Figure 4. Bitcoin: an interplay with technology, incentives and rules ......................... 10
Figure 5. Flavors of “Internet of Value” and blockchain applications ......................... 11
Figure 6. Merkle hashes .......................................................................................... 13
Figure 7. Coin is defined as a chain of digital signatures ........................................... 14
Figure 8. Illustration of “double spending” in P2P network ....................................... 15
Figure 9. Hash functions and proof of work, Block # 459900 on 2017-04-01 13:40:44, 16
Figure 10. Transaction costs must rise to maintain consistent miner compensation .... 19
Figure 11. Bitcoin price and hash rate ....................................................................... 20
Figure 12. Costless verification on a blockchain ....................................................... 21
Figure 13. Consensus in Bitcoin community ............................................................. 22
Figure 14. Different ledger technologies vary in “degree of centralization” ............... 24
Figure 15. Cost and Privacy trade-off of distributed ledger systems ......................... 26
Figure 16. The distributed ledgers taxonomy ............................................................ 27
Figure 17. Prison’s Dilemma Matrix – Nash equilibrium solution ............................... 28
Figure 18. The Business Logic with smart contract ............................................... 29
Figure 19. Smart Contracts are programs living on the blockchain ............................ 30
Figure 20. Schematic property title recordings on distributed ledgers ....................... 31
Figure 21. U.S. Structured Finance Issuance Volume ($ trillions) ............................... 33
Figure 22. Simplistic illustration of securitization structure ...................................... 34
Figure 23. Potential cost savings for mortgage lenders from the use of blockchain and smart contracts .......................... 37
Figure 24. Schematic review of securitization based on permissioned ledgers and smart contract ........................................ 39
A consensus means that everyone agrees to say collectively what no one believes individually.

Abba Eben

Introduction

On January 3, 2009, Satoshi Nakamoto published the genesis block of Bitcoin. Its coinbase parameter quoted a story in the Times of London newspaper on the same day headlined, “Chancellor on brink of second bailout for banks.” (Bitcoin.it, 2014) This might have been just a coincidence, but in the midst of a deeply mired financial crisis, this has been widely seen as revealing Satoshi’s motivation for the creation of Bitcoin and his note of disapproval on a centralized and mighty financial system that was dragging down the global economy.

The digital “peer-to-peer” payment protocol that Nakamoto invented has survived, thrived, and turned into a marketplace with an $18 billion value in a period of 8 years. Not only has Bitcoin gained over 13 million wallet users worldwide, but also the underlying public distributed ledger technology, commonly known as blockchain, has attracted massive interest and investments from the mainstream financial industry itself, which Bitcoin was meant to disrupt from the very beginning.

Janet Yellen, chair of the Board of Governors of the Federal Reserve System, recently called blockchain “a very important new technology” that “could make a big difference to the way in which transactions are cleared and settled in the global economy” (Young, 2017).

What has made Bitcoin and blockchain such a striking success story? In essence, Bitcoin’s achievement is due to an open-source technology that runs on a decentralized cryptographic database structure. It boils down to a fundamental question that Bitcoin tried to solve: How to create trust in the context of a trust-less financial community? Can technology become a way of establishing trust?

Blockchain, or the broader concept of distributed ledger technology (DLT), holds some interesting promise for these long-unsolved questions. It’s the first technology that has proven successful in digital payment by replacing trust with smart computation. Bitcoin embraced the concept of randomization,
and by this token established a novel mechanism to reach decentralized consensus on value, data, or anything that can be transferred to the distributed database system.

In this paper, we've tried to analyze the advantages and limitations of this decentralized consensus mechanism, especially in contrast to the traditional means of relying on a centralized trust intermediary, such as banks. To do this, we first have to go to a slightly technical level to fully appreciate the technology, and analyze its pros and cons. (Chapter 1). We argue that the choice of distributed ledger is a function of many variants, including complexity, degree of accessibility, existing level of trust, and the cost and benefit trade-off within the eco-system. The blockchain that underpins Bitcoin—although it remains the only proven one so far—might not be the universal one-size-fits-all solution for every business case. The choice of distributed ledger depends on the exact business context. (Chapter 2 and 3). We further demonstrate an example of asset securitization where the potential use-cases of distributed ledgers and smart contracts can apply (Chapter 4). In the end, we argue while distributed ledger technology is an impactful innovation, it's when it is combined with other technologies, like data analytics, artificial intelligence, and the Internet of Things, it may lead to real changes in the structure and nature of financial transactions in the digital age.

Throughout this paper I've found plenty of research that delved deep into the Bitcoin and blockchain systems, but less dealing with other distributed ledgers, particularly in areas of establishing and sharing common standards among them. That's probably because the other distributed ledgers technologies are still at a relatively nascent stage. In the area of applications, the majority of research has focused on digital payment, settlement, and clearing, and central banks' digital currencies, and less on smart contracts, digital marketplace, and supply-chain management, which attract a lot of interest from enterprises in digital transformations. These may represent areas for future research.
1. How Bitcoin Blockchain Achieved Decentralized Consensus

1.1 The Byzantine General's Problem

The challenge of reaching agreement among multiple members in a large system, where there is only limited trust between them, is well described by the so-called "Byzantine General’s Problem" (BGP), proposed by computer scientists first in 1982 (Lamport, Shostak, & Pease, 1982). Consider a group of generals camping around the enemy and having to rely on messengers to communicate among themselves to plan further actions. With the risk that some generals are "traitors" and some messengers can be intercepted, how could generals trust if the messages they receive in hand are indeed the "authentic" ones from their "good" counterparts? Could there be a robust algorithm that could be used to judge the generals' integrity? Scientists since have suggested that the distributed consensus is impossible to reach in one asynchronous fault-tolerant computational process (Fischer, Lynch, & Paterson, 1985).

The practical and convenient solution that society has depended on is to establish a central authority to intermediate as the agent of trust. The export and import industry is a good example. The importers will not necessarily trust that exporters will ship the goods if they've made the payment first; and the exporters will not trust the importers to be willing to pay after goods are delivered. Trust is about who moves first. Therefore, banks step in to intermediate the payment and document transactions as the third-party with neutral interests. Similarly in the case of sales and purchase of assets, or closing a house purchase, or obtaining mortgage, banks and lawyers play the intermediary role. There are plenty of cases in supply chain management like these. Generally, when there is a need to call in a deposit or collateral in order for the transaction to proceed, this is a clear sign that trust is missing and the transaction needs to be intermediated.

While a central institution can mitigate the trust problem, this, however, doesn't eradicate the root cause of mistrust. Having an intermediary creates new issues of inefficiency and information asymmetry, and most of all, the need for the entire system to trust the central authority. The possibility that the central institution might make errors and mistakes, or even engage in fraud and forgery, requires the centralized institution to make on-going reconciliation with other centralized institutions. This process...
leads to system bottlenecks and low efficiency. In addition, what if the central institution fails? The potential risk of a single point of failure also requires a lot of redundancy to be built to safeguard the system security. As a result, the added cost and expenses to maintain the centralized ledgers are carried by the entire system (DTCC, 2016).

1.2 The Bitcoin Success: Technology, Economics, and Rules

There have been plenty of efforts since the 1980s to address the intermediary issues, with particular emphasis on exploring innovations in the digital payment space. Most innovations have failed, however, with actually very few adoptions. PayPal is one of the few successful ones; it survived after quickly pivoting away from Cryptocurrency (Arvin, Bonneau, Edward, Andrew, & Steven, 2016). Thus, Bitcoin’s success can be seen as an extremely interesting and surprising achievement.

Under a pseudonym, Satoshi Nakamoto published the whitepaper, “Bitcoin: A peer-to-peer Electronic Cash System,” (Nakamoto, 2008) on the “cypherpunks” mailing list in 2008. Subsequently “he” established the initial Coinbase, hash, and the genesis block of Bitcoin on January 3, 2009 (Appendix: Figure 1). Over the next eight years, Bitcoin gradually attracted attention from millions of developers globally. As of April 3, 2017, there were 16.25 million bitcoins in circulation, with a total worth of around $18.7 billion USD in the global network. The price of a bitcoin has risen from initially nothing to now a historical high of about $1,327 on April 27, 2017, with roughly $373 million of daily turnover. (Figure 1)
How did Bitcoin achieve this success without a central governing authority? Blockchain emerged as the protocol backbone that has made Bitcoin possible. As suggested by the Google Trend statistics, since 2012 blockchain has attracted more interests than Bitcoin (Figure 2). Blockchain’s true potential is recognized for its wider applications beyond Bitcoin in cryptocurrency space. Since 2012, venture capital have poured in over USD 1.5 billion investments accumulatively in blockchain and Bitcoin (Figure 3). More than 2,500 Distributed Ledger Technology patents have filed since 2013, including many by financial institutions. (Project, Community, Part, & Series, 2016).
Bitcoin is an innovation story with many breakthroughs from the traditional centralized model. It incorporated the cryptographic proof instead of a central trust. It adopted a decentralized consensus algorithm to create trust in the network instead of in a central institution (William Mougayar, 2016). Brilliantly it introduced a smart incentive embedded in the technology, taking advantage of Bitcoin being a "currency" itself. As an open-source technology, Bitcoin has been attacked by all possible adversaries native to the internet and so far still proven to be amazingly robust. Bitcoin's success has been the result of an intricate interplay among three key factors: security of technology (blockchain), health of eco-system (mining), and the value of currency (Arvin et al., 2016) (Figure 4). The success of Bitcoin reveals a compelling bootstrapping process with strong economic network effects (Gandal & Halaburda, 2016).
1.3 Blockchain Technology - Consensus Without Identity

So what is blockchain? According to Goldman Sachs, the technology "has the potential to redefine transactions" and can "change...well everything" (Williams-Grut, 2015). McKinsey defined blockchain as the "cryptographic, or encoded, ledger comprising a digital log of transactions shared across a public or private network," and "one of the most disruptive innovations since the advent of the Internet." (McKinsey & Company, 2015). From Nakamoto's dis-intermediary value transfer network between peers, to consortia's digitizing development platform for enterprises (IBM, n.d.), blockchain can have multi-faceted meanings with distinct but complementary connotations: (William Mougayar, 2016)

- **Technology**: it's a distributed database that openly maintains a continuously growing list of ordered records called blocks (Wikipedia, 2017).
- **Business**: It's an exchange network for moving values between un-trusted peers.
- **Rules**: It's a decentralized, tamper-resistant validation framework, and a governance structure without a central authority.

Blockchain is partly database, partly development platform, and partly value network enabler. Just as the World Wide Web enables information flow with its technology standards on top of the internet, blockchain is a new construct of protocol that sits on top of internet and enables value possibly flow as freely as information currently does (Figure 5)(William Mougayar, 2016). Therefore many also consider blockchain to be the missing piece of the internet or the “internet of value” (Warner & Fox, 2015).

![Figure 5. Flavors of “Internet of Value” and blockchain applications](image)

*Adapted from “The Business Blockchain,” page 7, by William Mougayar*
Blockchain achieves value transfer on distributed ledgers through two major innovations. First, it validates transactions with cryptograph technology, primarily through hash functions and digital signatures. This validation is then implicitly enforced by consensus. Second, it protects against “double-spending,” almost entirely via consensus, which is based on a process of randomization named “proof of work” in Bitcoin. We will explain these two aspects separately.

1.3.1 Wallet: Validate with Hash Functions and Digital Signatures

For these value transactions on distributed ledgers, hash functions and digital signatures are the central attributes that provide security, anonymity and data integrity in absence of third-party validators.

**Hash Functions: Merkle tree and hash pointers**

Hash functions are deterministic models. Given an input, they generate a unique, fixed-length output (“digest”). Good hashing algorithms make intentional collisions virtually impossible. (Disrupter, 2016)

Bitcoin brilliantly adopts two different types of hash functions: hash transactions and hash chain data structure. Figure 6 is an example of hash transactions in Bitcoin Block # 459900, which was recorded on Blockchain at 13:40:44 on April 1, 2017.

This block included a digest of all 2,589 transactions by hashing pairs of transactions through a “tree,” and eventually all tied to the “root.” So the so-called “Merkle root hash” efficiently created a one single copy of “digest” for all transactions in the block. If any transaction is changed later, the hash changes too. It provides a finality and an audit trail for all transactions.

We’ll also notice each block has a few key attributes: a block header, a hash pointer to transaction data (Merkle root hash), and also a hash pointer referring to previous block in the sequence. Hash pointers not only provide the trails where and how this prior transaction comes from, but also verify if the contents of prior transactions are intact. By using the hash chain of blocks, Blockchain creates a public ledger system where databases are linked with hash pointers. (Nakamoto, 2008)

**Digital signatures: public key and private key**

Bitcoin uses a digital signature mechanism called ECDSA (Elliptic Curve Digital Signature Algorithm) (Bitcoinwiki, n.d.) to validate and confirm transactions. Each Bitcoin wallet contains a unique pair of public and private keys. Hashes are “signed” with private keys, and hashes are verified with public keys. As seen from
Figure 7, transactions transfer coins from an owner to a receiver by the owner signing hash of previous transaction and public key of next owner.

Digital signature hides the identities of the transaction counterparties. But the transaction is open for the public to see. Financial institutions and enterprises often have issues with this feature, because law and regulations often require them to protect customer confidentiality. Many other applications are trying to address this privacy issue; we'll discuss this in more detail in Chapter 2.

![Block #459,900](image)

Figure 6. Merkle hashes

Data source: Blockchain.info
Figure 7.
1.3.2 Network: a Consensus Mechanism against “Double Spending”

Using cryptography in digital payment is not Bitcoin’s innovation. David Chaum, known as the “father of digital currency,” invented the “Blind Signatures” in 1983 (“D. Chaum et al. (eds.),” 1983) and launched E-cash, which was regarded as the earliest form of digital currency. Even with some limited success, E-cash and many other digital currency inventions in the following twenty years, failed to solve the century-old double-spending problem: How to agree on the order of transactions, without necessarily relying on a central authority to serve as a time-stamper?

Take an instance: If Alice has $10, and she sends $10 to both Bob and Charlie via internet, then who can claim his $10 is legitimate? In the physical cash world this isn’t a problem because only one person holds the authentic bill. In the digital world however, both transactions would appear identical and equally valid. The best way to solve this is to order the facts, that is, the first $10 that gets recorded in the system becomes valid. Then how can the entire network beware and agree on the first fact? A consensus system is crucial. (Zaninotto, 2016)

Bitcoin solved this problem by effectively ensuring a process of randomization, namely “Proof of Work” (Nakamoto, 2008). A Proof of Work (PoW) is based on a competition of pure “luck” for solving the mathematical hash puzzle. Active servers on Bitcoin network keep incrementing a nonce until they find a hash of block. Because this is merely a process of computational iteration, finding the solution becomes a matter of effort, rather than mathematically ability. (Walport, 2015) This process of adding new transaction records to Bitcoin’s public ledger network is usually called “mining” and the servers or those who own those servers are referred to as “miners.” (“Bitcoin Mining,” n.d.) In fact, the probability of a
miner winning the next block is proportionate to its hash power in relation to that of global network. Once a hash function is solved, the miner becomes the time-stamper by adding the block to the chain, announcing to the entire network, and collecting the block rewards. (Malinova & Park, 2016)

This process is illustrated in Figure 9, a demonstration of hash functions and Proof of Work for the Bitcoin Block #459900 on April 1, 2017. Bitcoin adopts SHA-256, which is one of the more complex cryptographic hash functions. The previous block #459899 was added to the main chain at a time stamp of “2017-04-01 12:59:10.” It took the miners more than 40 minutes to find the next nonce, by a miner named “AntPool.” The miner eventually solved the block puzzle, added to the chain at the time stamp of “2017-04-01 13:40:44,” and claimed the Block Reward of 12.5 BTC.

![Figure 9. Hash functions and proof of work, Block #459900 on 2017-04-01 13:40:44. Data source: Blockchain.info](image-url)
Clearly for every double-spending transaction announced, there is competition among the community as to which one is to be added to the valid chain. Because of the latency, there is no guarantee that the one that got added is the “right” one. The longer the transaction is included in the longest chain, however, the safer it stays as a recognized transaction. In theory, there is no absolute guarantee, but normally after 6 blocks, the chance the first transaction is to be abandoned is reduced exponentially. On average six blocks takes about 60 minutes.

Figure 10 is a sample of above-described process with six blocks on April 1, 2017, from Block # 459900 to Block # 459905, running across a time span of around 40 minutes from “2017-04-01 13:40:44” to “2017-04-01 14:19:21.” The intervals between these blocks are quite random; sometimes it’s just 1 or 2 minutes, sometimes it is over 20 minutes. This interval varies because in the Bitcoin system the puzzle difficulty is adjusted automatically up or down to average out the intervals to about 10 minutes. In this specific sample, the miners who won the races of computation seemed very distributed.

It’s a fascinating game-theory process. According to Bitcoin protocol, only the longest chain is “valid” and miners get rewards only by appending blocks to this valid chain. Therefore when miners think about it, they have incentives to act in the “benevolent” way so that the rest of players would likely agree and append to the chain to which they’ve just done the work. Their chance is maximized by picking up and validating the “right” blocks and transactions in a very decentralized community, as long as the majority of players (more than 51 percent) are still honest.

It’s apparent that Proof of Work is a race in computation power. The winner “takes it all” so it can be argued that it’s a massive waste of time and energy for the rest of community overall. It’s the first time, however, a randomization process has worked to protect against the double-spending problem and it’s stood the test of time for the past eight years. Is there a better alternative to the PoW which would be effective but more economical? How much does trust need to cost to justify that PoW and other associated costs are worthwhile? There have been discussions about alternative consensus mechanism, such as Proof of Stake (PoS), which assigns users the shares of validation rights according to their stake in the system, (Walport, 2015). We’ll visit this question in Chapter 2.
Figure 10. Bitcoin Blockchain (Block #459900 – #459905) on April 1, 2017 (time stamp 13:40:44 - 14:19:21)

Data source: Blockchain.info
1.4 Economics – Miner’s Incentives

The consensus process plays an indispensable role in validating transactions and racing to build the chain of blocks. Why are miners motivated to do the work? Because there are two possible sets of payoffs for miners/validators.

1) Block reward: Miners are automatically paid with block rewards of newly “minted” coins when appending new blocks. Block reward started at 50 Bitcoins per block initially in 2009. By algorithm it automatically halves with every 210,000 blocks created, so roughly every four years based on current rate of block creation. The total expected maximum number of Bitcoin will reach 21 million in circulation in about 2040. In 2013 the block reward halved to 25 bitcoin per block after the total number of bitcoin in circulation reached 10.5 million. In 2016 the reward has halved again to 12.5 when the total bitcoin in existence reached 15.75 million. (Europe Central Bank, 2012) (Figure 11)

2) Transaction fees: Bitcoin transactions are wallet-based, meaning all “coins” are immutable and must be spent in their entirety in every transaction. So for every single transaction, the total inputs of unspent transactions (USPX) must be considered spent and equate to the total outputs. Any unspent output coin thus are picked up by miners as Transaction fees. Transaction fees have been minimal in the past but as block rewards get smaller, they might be more important to keep the total incentive at attractive levels. (Arvin et al., 2016) (Figure 11)

The price of bitcoin may also play a direct important impact on the incentives and hash rate (Figure 12). For example, between April 18, 2011, and July 19, 2011, Bitcoin price rose 13.55 times from $1.15 to
$15.59, and the network harsh rate increased 16.9 times from 661GH/sec to 11,188 GH/sec. This is a very smart incentive design on the part of Bitcoin. By algorithm the number of Bitcoin rewards reduces over time, but with more bitcoins in circulation the price will probably benefit from the increasing number of users and the growing acceptance of Bitcoin, this is called the network effect. The value of each bitcoin tends to rise with network effect so adequately offsets the decline in the number of rewards. For example, the total value of 12.5 bitcoin as block rewards on April 10, 2017, ($1227 per bitcoin) is worth a lot more than 50 bitcoin five years ago, when the price was $5.018 on April 18, 2012.

From blockchain users' perspective, if it inevitably becomes more expensive to reward miners to "mine" over time, why are users still interested in adopting blockchain? The answer is that blockchain can add enormous value by reducing two types of transaction costs significantly: the cost of verification and the cost of networking (Catalini & Gans, 2016).

Compared to traditional auditing or verification process via an intermediary, blockchain promotes data integrity via a system of ledger entries that are immutably linked in chronological order. The data-blocks that are linked by hash pointers not only provide the time-stamps of entire history of past transactions, but authenticate the transactions in real-time whether the information has remained intact by comparing the hash headers now and then. As a result, audit, verifications, or provenance tracking can be easily implemented at a minimum cost compared to traditional auditing (Figure 13).
Blockchain can also lower the network cost substantially. The computational power "investment" by miners in proof of work represents the economic sunk costs. Therefore miners are incentivized to behave in the "honest" manner so as to be picked up by the next miners then they stay on the longest chain to recoup the rewards.

The consensus process, with cryptography, Proof of Work and embedded incentive design, effectively replaces the cost of trust intermediation.

Financial service industry is a prominent example for which blockchain can generate significant value by improving transparency and cost efficiencies. According to a recent report by Accenture Consulting, by adopting blockchain infrastructure banks could potentially save 70% of current central reporting costs, 50% of business operations costs and 50% centralized operations costs, just to name a few. The annual cost reductions for eight of the world’s 10 largest investment banks can mount up to $8 billion to $12 billion (Accenture, 2015).

1.5 Rules – “Who is in Charge?”

Blockchain is an innovation based on a set of protocols: peer-to-peer networks, hash and digital signature cryptography, and decentralized consensus based on the resolution of a random mathematical challenge. None of these concepts are new. It’s their combination that allows a breakthrough in computing (Mougayar, 2017).
These rules are also written as part of, rather than separated from the technology. Together they serve the governance structure of the entire network: who has a final say on what and when? In the Bitcoin experiment, the community is comprised of developers, miners, investors, consumers, and users. They play by a rulebook, and there is a defined process to propose and discuss any changes (Arvin et al., 2016).

Some distributed technologies have features in common with Bitcoin Blockchain, but many others are different. In the long run, common standards become key. Sharing of these rulebooks will help develop quintessential standards for the technology. More about the Bitcoin community will be discussed in Section 5.

![Figure 14. Consensus in Bitcoin community](Adapted from Arvin et al., 2016)

### 1.6 The Consensus Mechanism

In short, a consensus mechanism is the process in which all or a majority of network validators come to agreement on the state of a ledger. (Swanson, 2015) It's a sum of rules and procedures that allow facts to be maintained cohesively and coherently among multiple participating nodes. The Bitcoin consensus, on the foundation of blockchain technology and incentive design, represents very significant case of decentralized consensus. Bitcoin Blockchain has its own limitations by design, such as the high cost of the proof of work, and the resulting slowdown of system, limited throughput, scale, and possible confidentiality issues. In the last few years multiple alternative consensus mechanisms have been developed in hopes of improving these challenging areas.
2. The Choice of Distributed Ledgers

2.1 Is it Possible to Separate Blockchain from Bitcoin?

The debate on the need of "tokenization" is not a new one. Many have liked blockchain but not necessarily the Bitcoin cryptocurrency. The question is: could a token-free blockchain be practical or possible at all without the unique censorship and decentralized security by proof-of-work?

To answer this, let's review the exact purpose of cryptocurrency. Bitcoin is named after "coin" but is only the unspent transactions (USPX). In fact, there is no such thing as "1 Bitcoin."(Arvin et al., 2016) It can be data, a medium of exchange, or anything with some intrinsic value. It's easier to think of Bitcoin as a public ledger system than as a physical currency. (DTCC, 2016) If people mine or purchase bitcoins, they don't receive any actual coins or tokens, instead they are given a slot in Bitcoin's ledger. Bitcoin wallets don't actually house bitcoins; they store the coin's private keys. Bitcoin is recording value because incentives are intricately engineered to reward the activities of validating and block extending.

So the question really boils down to the consensus algorithm – if there were no "tokens" on blockchain, who would decide on the blocks that form the chain. In a decentralized system, where there is no central authority to make this decision, Bitcoin embodies the rules of consensus. (Greenspan, 2015) As we've seen from last chapter, Bitcoin is a solution with technology inherently integrated with rules and economics.

Therefore the question whether Bitcoin needs to be divorced from blockchain is a fundamental question on consensus choice for the use-cases. Depending on how much trust currently exists in stakeholders in the ecosystem, and how much trust is needed, there is potentially a wide spectrum of technologies varying by the degree of trust, and needs for decentralization (Swanson, 2015) (see Figure 15).
On the left end of the spectrum, Bitcoin represents a completely “no trust,” decentralized, and by far the only proven model that was born native to the internet. There is no global Bitcoin market “open” and “close” time, it runs efficiently 24 hours a day, 7 days a week, and 365 days a year. It removes the needs for central intermediates. But cost of computing remains very high on a large scale, and confidentiality of the transactions remains an additional concern. (Tiller, 2015)

On the other end, traditional ledgers are centralized. They are proven and are still functioning reasonably well. But they are vulnerable to cyber-attacks and technology threats. They’ve evolved in the course of decades so have become increasingly complex over time, but they are poorly equipped to operate for 24/7/365 processing due to the pre-internet architecture design (DTCC, 2016). The systems are often very siloed with low transparency and multiple versions of truths, so there is a constant need to keep reconciling within the system and with other external systems. All these factors make centralized ledgers less secure, less efficient, and very expensive to maintain for today’s rapid changing market needs.

Between the two extremes, there are different modifications by the degrees of “decentralization.” Permissioned private ledgers only allows the pre-authorized nodes to access, read, write, and maintain an updated copy of each. These ledgers have no need for tokens, as they use permission-based access with certain levels of trusts. Thus the cost is low, security is high, but a certain degree of centralization is
still maintained. The public cannot either read or access. These can be represented by R3 CEV, Hyper-ledger or bank consortium.

Permissioned public ledgers allow “public” readers but only selected nodes as permissioned writers, and they generally still adopt tokens. This group can be represented by Ethereum or Ripple. (DTCC, 2016) Ethereum shares some commonality with Bitcoin. They are both about decentralizing trust, both have “blocks” of transactions linked together into a chain, and both use Proof of Work to reach consensus, though Ethereum plans to move to Proof of Stake in a future release (BlockCypher, 2017). But unlike Bitcoin which is wallet-based with USTX, Ethereum is account-based; it has a balance of each account number; and the system just stores a balance for each address, like a traditional bank might store the data. (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2015) The block time of Ethereum is 15 seconds, significantly shorter than Bitcoin, and its scripting language is more expressive than Bitcoin’s. More about Ethereum can be referenced through the Ethereum Wiki (Ethers, 2016).

2.2 Trade-off between Distributed Ledgers

In the end, the distributed ledger system is a network and a database. It provides the digital backbone to streamline business operations and validate data integrity with decentralized consensus. But confidentiality can be a major issue. If multiple institutions are using shared ledgers and seeing all the transactions, data privacy and security would be a great concern, both in terms of regulation and the commercial realities of competition. The choice of ledger is a trade-off, in which disintermediation is gained at the cost of confidentiality (Page, 2017b).

Figure 16 demonstrate such a balancing act. Bitcoin is completely decentralized, secure, most costly, and least private. Traditional ledgers are centralized, less secure, offers best secrecy but also high in cost. Compared to centralized ledger, permissioned private ledger is comparable in privacy protection but comes with major cost advantage. Compared with decentralized Bitcoin Blockchain, permissioned public is less costly and stronger in privacy protection.
Other important considerations involve speed, censorship, reversibility, and finality.

- **Node scalability**: how many nodes the DLTs supports without compromising performance? Permissioned DLTs typically offer sufficient client-node scalability with limited validation-node scalability.

- **Latency**: how long does it take to transact? Bitcoin Blockchain takes 10 minutes on average to validate and record transactions. Private DLTs without mining might offer sub-second latency level.

- **Throughput**: the number of transactions DLTs can take to process in a second. Bitcoin has incredibly low throughput of 7 tps (transactions per second); many other DLTs have made significant improvement on throughput, ranging from 500 to 5000 tps.

Distributed ledgers all have pros and cons on these dimensions. There is just no one size fits all. In general enterprises solutions tend to lean towards permissioned distributed ledgers as a “sweet spot” on all these trade-offs. Permissioned systems as a whole are capable of transacting faster and are cheaper to maintain than the capital-intensive permission-less systems. Permissioned distributed systems are also more congruent with existing centralized systems and therefore provide more utility to financial and enterprises institutions.
What does all this mean for business in practice? As suggested by the report from Government for Science in UK (Walport, 2015), it's good to run decisions through a flow of assessments and determine who can access the system, who is authorized to read, and who can write into the system, and the gap of trusts between the current and desired levels in the system. Distributed ledger technology is in essence the sum of all the rules reflecting such consensus. Getting all the stakeholders to agree to the "rights" and the governance structure might be one of the most challenging aspects of all in blockchain use-cases, particularly in forming multi-party consortia.

![Figure 17. The distributed ledgers taxonomy](image)

Adapted based on inputs from Consult Hyperion, page 19 (Walport, 2015)

### 2.3 Consensus: A Game-Theoretic View

From game theory perspective, human and organizations tend to cheat. Nash equilibrium suggests both parties choosing to defect, therefore, the "prison dilemma" (see below) empirically summarizes the sub-optimal efficiency of the mechanism. On Bitcoin Blockchain, consensus is based on computation with data transparency, immutability, and auditability. Miners act in the way to maximize their chances to be taken by other miners as "honest." This presents a very interesting field for future research on the intricate nature of consensus, but goes beyond the scope of this paper.
Figure 18. Prison's Dilemma Matrix – Nash equilibrium solution

<table>
<thead>
<tr>
<th>Player A</th>
<th>Player B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cooperate</strong></td>
<td><strong>Defect</strong></td>
</tr>
<tr>
<td>1 month in Jail (Reward for mutual cooperation)</td>
<td>Goes Free 1 Year in Jail</td>
</tr>
<tr>
<td>Defect</td>
<td>1 Year in Jail Goes Free</td>
</tr>
<tr>
<td></td>
<td>6 months in Jail (Punishment for mutual defection)</td>
</tr>
</tbody>
</table>
3. Beyond the Distributed Ledgers

3.1 Smart Contract

If distributed ledgers can digitize the business process and create trust and transparency in the deal chain, smart contracts would mean an opportunity to really re-imagine and transform the business. Smart contracts can be an innovative form to foster a more collaborative economy. The pre-coded arrangement can automate much complicate tasks among multi-parties beyond the capability of any singular organization. (Marvin, 2017)

In essence, smart contracts are the pre-agreed set of rules evaluated and executed by an automated system, where Blockchain essentially providing "adjudication-as-a-service," with added cryptographic mechanism for integrity (Marvin, 2017). Nick Szabo, who introduced the term “smart contract” in the paper, “Formalizing and Securing relationships on public networks” in 1990s (Szabo, 1994), once used the metaphor to describe a smart contract as a Blockchain-based “vending machine.”

The business logic is described in Figure 19 (Swanson, 2015) The contract is placed on autopilot on Blockchain. When the flow of events triggers the pre-set terms and conditions, the contacts will be activated; it'll read and write to internal storage, send other messages, or move contracts to the next stages.

![Figure 19. The Business Logic with smart contract](Source: Jo Lang/ R3 (Swanson, 2015))
Smart contracts could be flexible and replicable in terms and contracts, with all the “on-block” benefits of immutability and consensus properties of Blockchain. A close analogy is to think of Blockchain as distributed “OS”; then smart contracts are the “apps” on consensus. (Figure 20) Ethereum has tried to take this effort to the next level, building a program language that will make it easy to build a smart contract application.

How can transactions be animated to trigger future events? What tokens are transacted, are they native to the network? How do parties agree the ‘truth’ maintained in the shared ledger? How are transactions propagated within the network? Who has control over changes made to the shared ledger?

Flexibility
Innovation
Integrity
Robustness
Surety

Figure 20. Smart Contracts are programs living on the blockchain.
Source: Consult Hyperion, Credit Suisse Research (Disrupter, 2016)

3.2 Smart Property and IoT

In real business world, companies transact mostly in tangle, physical, real assets. The potential interaction between the physical “off-chain” assets with “digital assets” by coding “smart contracts” on blockchain gives rise to a concept called “smart property.”

An earlier version of “smart property” can be attributed to Nick Szabo in an example of a leased car. (Szabo, 1996) The car “key” can be a code or cryptographic PIN; when the car ownership is transferred, or the car lease payment is missed, the smart contract would automatically revoke the digital right to use of this car by disabling the private keys to unlock the car (Kelly, 2015).

How could this be possible in the digital space? Just as email allows us to send any messages to anyone connected to the internet, the rules prescribed by blockchain mean distributed ledgers can transfer anything of value securely connected.
Take the example of Bitcoin on public blockchain. As we have mentioned every “Bitcoin” is just unspent transaction outputs (UTXO). Every Bitcoin has an immutable history that anyone can view, validate, and audit in the open network. The fact that Bitcoin carries history means that bitcoins are not “fungible,” as we normally assume for currency. (Arvin et al., 2016) Every bitcoin is unique and special with its own history. If the cryptocurrency token is tagged to a certain piece of information, a two-dimension barcode can be a convenient form to reference and track that unique data movement on the blockchain. Figure 21 is an example how property titles can be digitalized and recorded on distributed ledgers.

![Figure 21. Schematic property title recordings on distributed ledgers](image)

The features of time-stamping and distributed consensus of distributed ledgers work well for managing the smart property. Consensus means that most nodes, either in permissioned or permissionless system, need to agree to the same piece of information. In this sense the sensor or IoT device can be controlled if it is connected to a distributed ledger-based network. Ethereum is working toward being such digital platform for the IoT (Loeb, 2015).

### 3.3 Build a Business Case with DLT

The distributed ledger technologies and smart contracts are not panacea for all the information problems. In fact, not many business even need to use DLT in the first place. As some have argued, DLTs can be “over-hyped.” DLTs provide the powerful and alternative solutions for disintermediation and consensus, but these come at costs.

To take advantage of DLTs, business situations first shall require a shared database. Otherwise, as Figure 17 suggests, the traditional centralized ledger might just work fine. Secondly, the system requires multiple writers to contribute to modify the database, but there is not necessarily much trust among them. Third, there is a strong need for disintermediation and there are some inter-dependence of
actions between the transactions created by these writers (Page, 2017a). In these situations distributed ledgers truly outshine.
4. Securitization: Potential Use-cases of DLTs

4.1 How Securitization Works

One of the biggest innovations to the credit markets of the last century was the securitization of debt obligations and the development of all the myriad derivatives one can see in the market today (ETHereal, 2015). Securitization is the issuance of marketable securities backed by the expected cash flows from specific assets (receivables). In the United States, securitization issuance, including agency and non-agency mortgage-backed securities (MBS) and asset-backed securities (ABS), totaled $2.2 trillion in 2016, accounting for about 30% of total funding in capital market, even though that is down from a 60% peak level prior to the 2008 finance crisis. (Adelson & Conner, 2017) Securitization represents an important financial means to support the real economy by re-allocating risk and capital through the modern capital market. (Wall, Richardson, Bowkett, & Llp, 2017)

![Figure 22. U.S. Structured Finance Issuance Volume ($ trillions)](image)

Figure 23 illustrates how a typical securitization works, in highly simplified terms:

1) The first step of securitization (flow 1-5) starts by sponsors “pooling” a suitably large portfolio of financial assets and transferring this “asset pool” to a Special-Purpose Vehicle entity (SPV), a bankruptcy remote entity—to legally isolate the assets. SPV then structures the claims to future cash flow (receivables generated by the assets) into “tranches” of securities with distinct risk-
return profiles. SPV obtains credit ratings for these different securities and sells them to investors. Conversely, the SPV also conveys the capital it receives from investors back to the issuer.

2) Arrangers, typically investment banks, help with entire deal structuring, making arrangement on credit and liquid support if necessary, and coordinating the subscription of securities. The issuer is often required to retain some portion of the asset backed securities (ABS) or other contractual interests (e.g., servicing rights and recourse obligations).

3) Subsequently (flow 6-7) SPV forwards the cash received from collection agents (often also Issuers) to investors, issuers and any other third-party guarantors.

In short, securitization represents an essential financial tool in modern credit market. It de-links the credit risk of assets from the credit risk of the originators, and by converting the assets into layered securities, creates liquidity from illiquid assets. Securitization normally helps issues to get a cheaper funding for it reduces an asset's credit risk premium. Investors also benefit with the expanded access to the products with differentiated risk profiles. As seen from Figure 23, every securitization transaction requires close collaboration of multiple players along the "value chain." They share a large amount of asset data in decision-making and also contribute inputs from their own way. Their strong cooperation is needed to ensure data transparency, accuracy, and authenticity.
4.2 How DLT Helps Securitization

Post financial crisis, the securitization market in the United States took a deep dive in both market issuance and market liquidity. As shown in Figure 22, the market has since gradually recovered but still well below the peak levels preceding the financial crisis. The market has focused on the compliance and risk management under prudence requirement in regulation and legislation (Segoviano, Jones, Lindner, & Blankenheim, 2015). The key regulation changes include:

- **Risk retention:** *Dodd-Frank* established a requirement for a sponsor of securitization to retain no less than 5% of the aggregate credit risk of assets, either via a vertical retention, 5% of each tranche; or a horizontal retention, 5% of ABS first-loss position (or fully funded horizontal cash reserve account); or a combination of the two methods. It can take less than 5% retention for an asset if the originator meets the prescribed underwriting standards that indicate a low credit risk. The risk retention regulations became effective for CMBS on December 24, 2016.

- **Capital and liquidity regulation (BASLE III):** A comprehensive understanding of the features of a securitization, including performance of the position is required pre-trade, in addition to post-trade (T+3) documentation and quarterly reviews. 100% of the undrawn amount of all committed credit and liquidity facilities extended to special purpose entities (SPEs) be included in the LCR calculation.

- **Regulation AB II:** SEC requires to institute loan-level disclosure requirements to investors and credit agents, for public issued ABS and privately issued structured finance products.

These market regulations have aimed to reform the system and restore a sound governance framework with data integrity and transparency. With distributed consensus and immutable record keeping, capability distributed ledgers can crystalize the overburdened point-to-point communications among market players. Competing financial institutions would be able to share a common digital representation of asset holdings and to keep track of the origination, execution, and settlement of the securities transactions. In addition, smart contracts could automate the interactions between players and manage the risks and assets in a precise manner in accordance to the pre-coded terms, without the need to involve a central database management system. (Walport, 2015)
Table 1. Areas that would benefit from the adoption of distributed ledgers

<table>
<thead>
<tr>
<th>Securitization Practices</th>
<th>Challenges</th>
<th>DLT solutions</th>
</tr>
</thead>
</table>
| 1. Due Diligence Items:  | - Difficulty and latency to obtain real-time readings on lien positions and property value changes.  
- The crisis-period troubles were primarily associated with these issues in RMBS products.  
- State of these loan performance info is locked away in organizational silos, loosely kept. | DLT can provide real-time information from updates from title registration and market transactions.  
Information updated simultaneously to all parties end-to-end in the system  
Single source of truth to all parties  
Real time: 24/7/365 |
| 2. Loan-level data management | Large amount of loan-level data has not customarily been available to investors or rating analysis of an asset class.  
- Difficulties in tracking and safekeeping large amount of data  
- High cost in maintenance | DLT would make it possible to track critical information like defaults, lien perfection status, defaults, late payment, interest rates, and amortization types, for individual assets as well as tiers of securities. |
| 3. Risk retention | Expensive to maintain and keep data recordation to auditor’s and investor’s requests.  
- Very manual based and huge operational inefficiency | Risk retention requirement would be coded in the securities structure, and automatically executed.  
create a tamper proof evidence |
| 4. Payment Waterfall | Still very manual and paper-based process  
- Error prone, which requires constant reconciliation | Payment waterfall will be automatically triggered and executed once payments are received. |
| 5. Marketplace investing | Liquidity has suffered due to low confidence from investors | Provide data transparency, and authenticity with faster feedback and lower latency |
| 6. Equipment ABS | Technology remains a focus in both the small and large equipment ends of the sector. | DLT tracking with Smart Contract |

Distributed ledgers technology represents an intriguing option for market players to stay agile to ever-changing market condition and compliance requirements, and improve on huge operation inefficiency currently in the system. Decentralized data access and transparency would restore investor’s confidence and help attract the market liquidity.
Take the example of mortgage loan origination process. Regulation AB II requires loan-level data management. Figure 24 illustrates the process of individual loan-level data collection, complexity in large categorical data repository, tracking, and safekeeping.

According to Capgemini Consulting reporting, the current costs of mortgage loan origination in the United States stand about USD $17 billion. The potential cost saving from the use of blockchain and smart contracts can be a range of $1.5 billion to $6 billion, a whopping 9% to 35% of cost reduction (Capgemini Consulting, 2016).

In fact, all loan information relies on the accuracy of underlying source data. Blockchain can help validate and maintain the integrity of mortgage loan data and other documents, making it easier to transfer assets to servicers.

A securitization project on the distributed ledger/smart contracts may work (Figure 25).

- First, every single underlying asset can be assigned a digital identification, for example, immobilizer automobile, house, and equipment. When the digital ID is logged in the central ledger, all the underlying
data, including title, registration of deed, lean condition, and ownership transfer of such assets, would be available for all authorized users to access. This would create one single record of truth, and auditable trail of changes for each asset.

- At origination, distributed ledgers might help establish accurate recordkeeping. Large amount of asset-level data would be collected and made accessible for sponsors, arrangers, credit agents, and authorized investors to see and analyze. At fulfillment, it could provide immutable proof that loan estimates are up-to-date. Smart contracts would streamline and speed up settlement flows.

- After asset pooling, loan-level data are still monitored and kept up-to-date. If certain assets are changed, e.g., title transfer, repayment, or even at default, the status is updated for all to see. Latency in communication would be reduced. Credit analysis would be updated simultaneously on the impacted “tranches” of securities, and all can be traced back to the source of change in asset characteristics any time.

- In the loan-servicing process, blockchain could track the movement of payments. And in the secondary markets, it might provide transparency about the ownership of underlying assets. If a certain loan is at default, it'll automatically trigger the collateral liquidation process programmed in the smart contract. The smart contract will initiate asset auction, transfer title to new owners, and take payments.

- In the securities servicing process: smart contracts can digitize the payment flow in accordance with the pre-scribed waterfall mechanism. Risk retention of sponsors are automatically adjusted. No manual operation or human intervention is needed. This would also reduce the risk of forgery and fraud.
In summary, all actions related to the documents and cash flows are captured and shared: which payments are submitted when and by whom, where they are, and who is in possession of them and the next steps in the process. Once a payment is collected/missed by collection agent, simultaneously the information is communicated to allow the downstream players to start preparing the receiving of values. The DLT is real time, 24/7/365, so there are no delays or missteps. Blockchain provides secure data exchange and a tamper-proof repository for documents and events. This could significantly reduce the delays and save billions of dollars annually.
5. Looking Forward: Is DLT Really “a Solution Looking for a Problem”? 

Blockchain and distributed ledger technology have generated much excitement in recent years. There have been plenty of academic studies, industry consortia, and even proofs-of-concept floating around, and few, if any, production-ready software systems. Bitcoin as of this date is still the only proven application on the blockchain. Hence there are also debates and skepticism about the real applications of blockchain; some question if it’s pre-mature or over-hyped, and others suggest many proposed applications are either “naive or miss the mark outright” (Lipton, 2016). In a nutshell, the question is how likely is blockchain to produce a real revolution? Or is it just a solution looking for a problem? 

As we have already learned, blockchain technology is a way to maintain information in a secure distributed ledger. Blocks are managed in chronological order with cryptographic security. By eliminating the need for a trusted intermediary, blockchain brings about reliability, immutability, transparency, and cost efficiency. Therefore businesses that deal with slow, costly, or unreliable transactions, have good reasons to consider distributed ledger technology. Then how can we get blockchain to a stage where it can be usefully applied? 

It’s always helpful to visit the case of Bitcoin. Bitcoin has lived through an amazing bootstrapping journey and stood the test of time. In fact, the year 2017 has been a year of continuous new historical highs of bitcoin prices despite all the skepticism. On May 4, 2017, Bitcoin was trading over $1537 (Blockchain.info, 2017); as a reference, Gold at spot market closed at $1228 per ounce (Bloomberg, 2017). What has made 1 unit of Unspent Transaction Output (UTXO) of bitcoin worth more than one ounce of gold, in value perceived by market participants? What has made Bitcoin work in contrast to other applications? 

In Chapter 1 we discussed how Bitcoin is an intricate interplay among three key factors: technology (blockchain), incentives, and the rules of the eco-system. The success of Bitcoin is more than a story of technology; it is also a smart engineering of incentives with deep insights into human behavior in the
context of networking (consensus). The Bitcoin assets are built-in as part of the technology itself. Incentives and rules are not separable from technology but all three attributes constitute the formation of Bitcoin. That’s how Bitcoin survived the pitfalls of earlier cryptocurrencies. Bitcoin protocol had a very special and clever design from the very beginning.

Agreeing to a rulebook among community participants on an open public platform is never easy, if not nearly impossible. Bitcoin had the advantage of a convenient start, in that Satoshi Nakamoto wrote the original codes by himself. In the next three years, he and a group of developers maintained the Bitcoin Core, the open-source software that is a focal point for discussions and debates about Bitcoin rules. Now Nakamoto is no long active, the core developers, namely a handful who have direct “commit” access to the Core repository, continuously lead the way for community to improve the Bitcoin Core. It's the most widely used Bitcoin software and many alt-coins have just mimicked its rules. The rulebook has a process called “Bitcoin Improvement Proposals” (BIPs) for anyone to contribute, propose, and specify any changes.

We discussed the question “Who is in charge?” in Section 1.5. It's fascinating to note that within Bitcoin community the power is quite distributed and balanced. On first glance, Core developers have strong power because they write the rules. But if there is a good amount of disagreement on how rules are enforced, developers can simply “hard fork,” that is, to start a new genesis block and start a new chain. Miners have power too, because they write the history and decide which transactions and blocks are valid. Investors also have power, because they determine the value of the Bitcoin, and without such value miners wouldn’t even be motivated to “mine” the blocks so the integrity of the entire data system could be at risk. Payment agents, merchants, and customers have power because they are the ultimate users of Bitcoins. This is a very delicate balance of power among different groups (Arvin et al., 2016).

Why does this make sense? It's because the decentralized protocol still represents a relatively new and unfamiliar governance model for other blockchain applications. It's interesting to observe how Bitcoin’s internal politics have evolved, and how they have ultimately interacted with traditional politics, namely law and regulations. This dynamics could offer valuable insights that benefit various DLTs in developing future applications.
Clearly DLT is not just a technology, nor simply just a technology looking for a solution. It's a technology with pre-coded incentive mechanisms and represents a decentralized governance model. A business use-case running on top of blockchain and DLT needs to consist of the standards and rules for every node to agree and apply, including how to share information, who verifies the data integrity, and who gets rewarded for how much worth on what can be considered “honest” behaviors. This could be a massive, complex, and sometimes messy and ugly consensus-building exercise, in a decentralized setting.

For enterprise solutions, this could require the business partners, either internally within organizations or externally across supply-chain or other forms of partnerships, to re-design the existing governance process to rely on a new set of architectural principles that need continuous reviews. For most current blockchain consortia, this means they'll need to work on all different levels of partnership in information sharing, censoring, and controlling. Compared to the past cooperation models among corporations that are either “make” or “buy,” the new partnerships require each involved unit to reduce information silos, to empower and be held accountable in a more decentralized way, and adopt a new different trust relationship. Are the current corporations ready?

As we have seen in recent development in enterprise DLT consortia, building a “proof of concept” can turn out to be a relatively straightforward beginning. But the “proof of concept” wouldn't necessarily suggest what pieces of it would get buy-in from which customers, and how easy or difficult to scale. It'll take significant efforts to align counterparties’ interests, and often demand superior business and negotiation skills that can go well beyond the developers’ expertise in technical domain. It's not a simple, quick process nor a task to take lightly. That's partially why the majority of “proofs of concept” have struggled.

Even in the case of Bitcoin, it's not always a smooth sailing process. Recently there have been heated debates within the Bitcoin community on how to scale up Bitcoin's capacity, as by Nakamoto’s original rule every block has a size limit of 1 megabyte. This limit imposes significant constraints on Bitcoin processing capacity as Bitcoin has gained more popularity. With increasing amount of transactions flowing through the network, this limit has caused delays for transactions to be included in the chain. This has been a long nagging issue, but recently heated up partly triggered by US SEC’s rejection of a possible Bitcoin EFT. The group who sees Bitcoin as an investment and the group who uses Bitcoin as a payment tool have very distinct views on how the rules should be revised going forward. The differences
are ideological and there has been little consensus in sight. Risk of hard-forking is serious as the Bitcoin "civil war" is still evolving (Williams-Grut & Price, 2017).

A decentralized governance model empowered by the decentralized, internet-native DLT may lead to a new dimension of organizational changes. In the last two centuries modern organizations have brought about significant societal advancement but seem to have been "stretched to their limits." The breakthroughs in organization reinvention may take the form of operating on a basis of peer relationships rather than hierarchy, involving much higher level of self-management, wholeness, and evolutionary purpose (Laloux, 2014).

As pointed out in the recent report from World Economic Forum, more than 90 corporations have joined DLT consortia, 80% of banks are predicted to initiate a DLT project by 2017, and more than 90 central banks are engaged in DLT discussions (World Economic Forum, 2016). Changes may take time, and in particular, international and domestic financial regulations will need to play an instrumental role in reshaping the rules and standards to foster innovation in the financial services. But collaboration and cooperation are key to the future. With the promise of a vast cost reduction in validation and networking (Catalini & Gans, 2016), distributed ledger technology could represent a defining moment for innovations in financial services (Wilkins, 2016), and for interests and imaginations beyond the financial services industry.
6. Conclusion

Historians believed that the critical ability of Homo Sapiens to think abstractly and act collectively via common beliefs in “fictions” accounted for their success in combatting other human species for the dominance on earth in prehistoric times. Common beliefs initially took the form of religion, and later of money, the shared medium of exchange, or the “currency” (Harari, 2015).

Common beliefs matter even more in today's digital age, when we often have to make prompt and critical decisions based on our faith in one single version of “truth” among individuals, institutions and society. Wouldn’t it be great if the society had a set of common standards and rules for exchanging value and information, agreeing on the data integrity (proof of work) and creating incentives for trustworthy behaviors (consensus model)? That’s why the emerging blockchain technology and DLTs seem so intriguing and exciting.

The intention of this paper is to evaluate the consensus framework that Bitcoin, blockchain and other DLTs may have brought to us, and to bring forward some thinking on future applications. The concept of disintermediation through decentralization is deep, novel, and fascinating. The future of DLT is not just about how these technological protocols might evolve. It's a new way of trust building, a different way of thinking about forming institutional relationships via the power of decentralization, as in, for example, Decentralized Autonomous Organizations (DAOs).

We should recognize, however, that DLT is still at a very nascent stage and will continue to struggle with many challenges. Complying with the regulations, or the lack of them in some circumstances, represents an ongoing risk, just as with any other innovations. The discussions on common standards and inter-operability among different DLTs still seem very opaque and we’re a long way from reaching an agreement.
While changes are always difficult, we live in a time with innovations happening at exponential speed. The future power of DLT, or other form of decentralized data technologies, lies in its promise for working with and unlocking the full potentials of many other technologies, such as artificial intelligence, data analytics, and IoT. It’s due to a revolution of technology whose time has come (Masters, 2016).
## Appendix

### Genesis Block, posted by Satoshi Nakamoto in Jan 2009

Block Height 0 Blocks at depth 0 in the bitcoin blockchain

<table>
<thead>
<tr>
<th>Summary</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>0 (Main chain)</td>
</tr>
<tr>
<td>Hash</td>
<td>000000000019d6689c0850e188a6e46f47276f5d5e0b0e2fa6f</td>
</tr>
<tr>
<td>Previous Block</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>Next Blocks</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>Time</td>
<td>2009-01-03 18:15:05</td>
</tr>
<tr>
<td>Difficulty</td>
<td>1</td>
</tr>
<tr>
<td>Bits</td>
<td>4866047959</td>
</tr>
<tr>
<td>Number Of Transactions</td>
<td>1</td>
</tr>
<tr>
<td>Output Total</td>
<td>50 BTC</td>
</tr>
<tr>
<td>Estimated Transaction Volume</td>
<td>0 BTC</td>
</tr>
<tr>
<td>Size</td>
<td>0.285 KB</td>
</tr>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Merkle Root</td>
<td>4a5e1e4bbae89a325189bc31bc8761f6973e2c77e6217b7af0a9da339</td>
</tr>
<tr>
<td>Nonce</td>
<td>2083206893</td>
</tr>
<tr>
<td>Block Reward</td>
<td>50 BTC</td>
</tr>
<tr>
<td>Transaction Fees</td>
<td>0 BTC</td>
</tr>
</tbody>
</table>

Source: Blockchain.info. Coinbase.
References


https://doi.org/10.1057/palgrave.jit.2000080


https://doi.org/http://dx.doi.org/10.2139/ssrn.2874598

D. Chaum et al. (eds.),. (1983), 199(2), 199–203.


